Massive cyberattack shuts down large sections of the Internet

Kevin Reed
22 October 2016

Websites around the globe became inaccessible on Friday when the servers of Dyn—a major US provider of services that direct Internet traffic—were disabled by multiple and internationally coordinated distributed denial of service (DDoS) attacks. Located in Manchester, New Hampshire, Dyn began reporting that a cyberattack had hit its domain name system (DNS) infrastructure on the east coast of the US at around 7:10 a.m. Friday.

The outage—which spread across the US in three waves throughout the day—impacted popular sites such as Amazon, Twitter, Spotify, Netflix, PayPal and Reddit as well as the *World Socialist Web Site*. The sites were shut down for hours at a time as users and readers were unable to login to their accounts or gain access to web pages from their browsers and mobile devices.

The DNS services provided by Dyn and others are critical to the operation of the World Wide Web. The servers perform the function of translating a named web address—entered as a URL such as "wsws.org" in a browser, for example—into the numeric, machine readable Internet (IP) address that identifies the actual web server on the Internet. A DDoS attack overwhelms the targeted DNS server with such large numbers of requests that it gets bogged down, becomes inoperable or crashes.

While DDoS attacks are not uncommon today, in this particular case the assault was very large in scale and sophisticated in coordination. According to Dyn representatives, the cyberattack came from tens of millions of Internet locations internationally and arrived in three waves: 7a.m., just before noon and a little after 4 p.m.

Kyle York, Dyn's chief strategist, told the *New York Times* that his and other DNS host companies have been the target of increasingly powerful attacks. He said, "The number and types of attacks, the duration of attacks and the complexity of these attacks are all on the rise."

Several media reports said that Friday's attack likely included so-called "Internet of Things" technologies such as smart appliances, webcams and DVRs that had been infected by malware and converted into an army of remotely-controlled cyber assault devices called a botnet. Although no specific or definitive evidence has been presented, it is being suggested that the scale of the assault could only have been carried out if the DDoS hackers had commandeered such malware infected devices and pointed them at the Dyn servers.

PopularMechanics reported that the botnet issue has been building up for months prior to Friday's attack. Earlier in October the source code for the Mirai botnet—malware specifically targeting poorly secured "Internet of Things" devices—had been released on the web. It is known that the biggest ever DDoS attack took place last September and was mounted by devices compromised by Mirai.

Major news outlets are reporting that the FBI and Department of Homeland Security are investigating the outage and determined that it was the result of a malicious attack. They are treating it as a criminal act or "an act of state sponsored cyberwarfare." According to a report in the *L os A ngeles Times*, an anonymous federal law enforcement official said: "Investigators have come to a preliminary conclusion as to who carried them out, but are not planning to make that public for now."

The Dyn attack follows a number of recent events that have pointed to the vulnerability of Internet technologies to coordinated cyber assault, as well as the attempts by the US ruling establishment to use these

developments for their own political and military purposes. The appearance on WikiLeaks of the hacked private email of Hillary Clinton’s campaign chairman John Podesta has been blamed on Russia by both the Democratic Party leadership and much of the capitalist media. Meanwhile, the recent announcement that 500 million Yahoo email accounts were hacked in 2014 was also charged to an unnamed “state-sponsored actor.”

It is a well-established fact that the US government and its state-within-the-state organizations, such as the NSA, are responsible for the majority of the world’s cyberespionage and illegal malware activity. There is every reason to expect an increase in incidence of cyberwarfare as a component part of plans to ramp up militarism abroad and attacks on democratic rights at home after the November 8 elections.