The New York Times | http://nyti.ms/2ep3v2m

TECHNOLOGY

Hackers Used New Weapons to Disrupt Major Websites Across U.S.

By NICOLE PERLROTH OCT. 21, 2016

SAN FRANCISCO — Major websites were inaccessible to people across wide swaths of the United States on Friday after a company that manages crucial parts of the internet's infrastructure said it was under attack.

Users reported sporadic problems reaching several websites, including Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud and The New York Times.

The company, Dyn, whose servers monitor and reroute internet traffic, said it began experiencing what security experts called a distributed denial-of-service attack just after 7 a.m. Reports that many sites were inaccessible started on the East Coast, but spread westward in three waves as the day wore on and into the evening.

And in a troubling development, the attack appears to have relied on hundreds of thousands of internet-connected devices like cameras, baby monitors and home routers that have been infected — without their owners' knowledge — with software that allows hackers to command them to flood a target with overwhelming traffic.

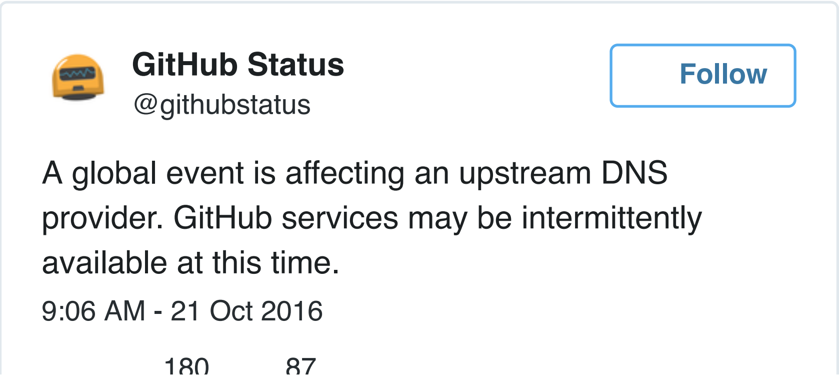
A spokeswoman said the Federal Bureau of Investigation and the Department of Homeland Security were looking into the incident and all potential causes, including criminal activity and a nation-state attack.

Kyle York, Dyn's chief strategist, said his company and others that host the core parts of the internet's infrastructure were targets for a growing number of more powerful attacks.

“The number and types of attacks, the duration of attacks and the complexity of these attacks are all on the rise,” Mr. York said.

Security researchers have long warned that the increasing number of devices being hooked up to the internet, the so-called Internet of Things, would present an enormous security issue. And the assault on Friday, security researchers say, is only a glimpse of how those devices can be used for online attacks.

Dyn, based in Manchester, N.H., said it had fended off the assault by 9:30 a.m. But by 11:52 a.m., Dyn said it was again under attack. After fending off the second wave of attacks, Dyn said at 5 p.m. that it was again facing a flood of traffic.



GitHub Status
@githubstatus

A global event is affecting an upstream DNS provider. GitHub services may be intermittently available at this time.

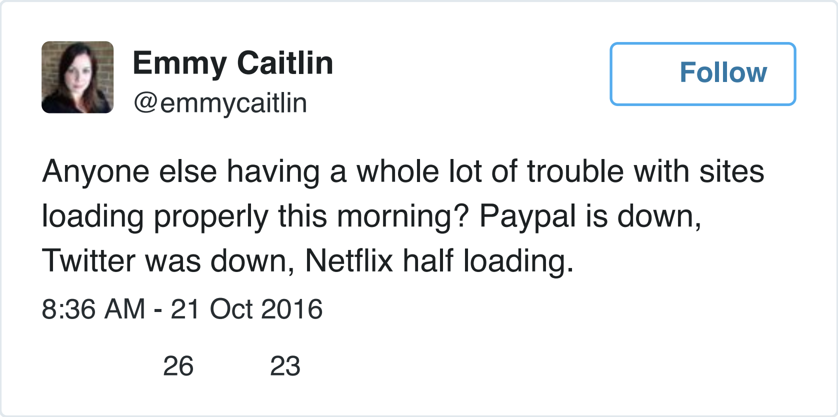
9:06 AM - 21 Oct 2016

A distributed denial-of-service attack, or DDoS, occurs when hackers flood the servers that run a target’s site with internet traffic until it stumbles or collapses under the load. Such attacks are common, but there is evidence that they are becoming more powerful, more sophisticated and increasingly aimed at core internet infrastructure providers.

Going after companies like Dyn can cause far more damage than aiming at a single website.

Dyn is one of many outfits that host the Domain Name System, or DNS, which functions as a switchboard for the internet. The DNS translates user-friendly web addresses like fbi.gov into numerical addresses that allow computers to speak to one another. Without the DNS servers operated by internet service providers, the internet could not operate.

In this case, the attack was aimed at the Dyn infrastructure that supports internet connections. While the attack did not affect the websites themselves, it blocked or slowed users trying to gain access to those sites.



Emmy Caitlin
@emmycaitlin

Anyone else having a whole lot of trouble with sites loading properly this morning? Paypal is down, Twitter was down, Netflix half loading.

8:36 AM - 21 Oct 2016

Mr. York, the Dyn strategist, said in an interview during a lull in the attacks that the assaults on its servers were complex.

“This was not your everyday DDoS attack,” Mr. York said. “The nature and source of the attack is still under investigation.”

Later in the day, Dave Allen, the general counsel at Dyn, said tens of millions of internet addresses, or so-called I.P. addresses, were being used to send a fire hose of internet traffic at the company’s servers. He confirmed that a large portion of that traffic was coming from internet-connected devices that had been co-opted by type of malware, called Mirai.

Dale Drew, chief security officer at Level 3, an internet service provider, found evidence that roughly 10 percent of all devices co-opted by Mirai were being used to attack Dyn’s servers. Just one week ago, Level 3 found that 493,000 devices had been infected with Mirai malware, nearly double the number infected last month.

Mr. Allen added that Dyn was collaborating with law enforcement and other internet service providers to deal with the attacks.

In a recent report, Verisign, a registrar for many internet sites that has a unique perspective into this type of attack activity, reported a 75 percent increase in such attacks from April through June of this year, compared with the same period last year.

The attacks were not only more frequent, they were bigger and more sophisticated. The typical attack more than doubled in size. What is more, the attackers were simultaneously using different methods to attack the company's servers, making them harder to stop.

The most frequent targets were businesses that provide internet infrastructure services like Dyn.

"DNS has often been neglected in terms of its security and availability," Richard Meeus, vice president for technology at Nsfocus, a network security firm, wrote in an email. "It is treated as if it will always be there in the same way that water comes out of the tap."

Last month, Bruce Schneier, a security expert and blogger, wrote on the Lawfare blog that someone had been probing the defenses of companies that run crucial pieces of the internet.

"These probes take the form of precisely calibrated attacks designed to determine exactly how well the companies can defend themselves, and what would be required to take them down," Mr. Schneier wrote. "We don't know who is doing this, but it feels like a large nation-state. China and Russia would be my first guesses."

It is too early to determine who was behind Friday's attacks, but it is this type of attack that has election officials concerned. They are worried that an attack could keep citizens from submitting votes.

Thirty-one states and the District of Columbia allow internet voting for overseas military and civilians. Alaska allows any Alaskan citizen to do so. Barbara Simons, the co-author of the book "Broken Ballots: Will Your Vote Count?" and a member of the board of advisers to the Election Assistance Commission, the federal body that oversees voting technology standards, said she had been losing sleep over just this prospect.

"A DDoS attack could certainly impact these votes and make a big difference in swing states," Dr. Simons said on Friday. "This is a strong argument for why we should not allow voters to send their voted ballots over the internet."

This month the director of national intelligence, James Clapper, and the Department of Homeland Security accused Russia of hacking the Democratic

National Committee, apparently in an effort to affect the presidential election. There has been speculation about whether President Obama has ordered the National Security Agency to conduct a retaliatory attack and the potential backlash this might cause from Russia.

Gillian M. Christensen, deputy press secretary for the Department of Homeland Security, said the agency was investigating "all potential causes" of the attack.

Vice President Joseph R. Biden Jr. said on the NBC News program "Meet the Press" this month that the United States was prepared to respond to Russia's election attacks in kind. "We're sending a message," Mr. Biden said. "We have the capacity to do it."

But technology providers in the United States could suffer blowback. As Dyn fell under recurring attacks on Friday, Mr. York, the chief strategist, said such assaults were the reason so many companies are pushing at least parts of their infrastructure to cloud computing networks, to decentralize their systems and make them harder to attack.

"It's a total wild, wild west out there," Mr. York said.

Erin McCann contributed reporting from New York.

A version of this article appears in print on October 22, 2016, on page A1 of the New York edition with the headline: New Weapons Used in Attack on the Internet.