Maybe 100,000 hijacked devices used in cyber attack: Dyn

October 26 2016

US Director of National Intelligence James Clapper, seen in September 2016, said he believed a "non-state actor" was behind last week's cyber attack on Dynamic Network Services Inc, or Dyn

The US company targeted in last week's massive cyber attack said Monday that possibly 100,000 connected devices were hijacked to swamp its systems and close off the internet to millions of users.

Dynamic Network Services Inc, or Dyn, said it was cooperating in a criminal investigation into the incident and "will not speculate regarding the motivation or the identity of the attackers."

But it said it had identified a notorious botnet, Mirai, as the primary tool in surreptitiously marshalling a huge number of internet-linked devices like cellphones, printers and security cameras to mount the "complex & sophisticated" attack.

Friday's attack overwhelmed Dyn's central role in routing and managing internet traffic, making it hard for millions of people to access popular sites like Amazon, Twitter and Netflix.

Government officials have commented little on the attack, which raised important national security issues. On Monday Director of National Intelligence James Clapper said an investigation was underway, but added that the government believed a "non-state actor" was behind it.

"But I wouldn't want to be conclusively definitive about that yet," Clapper said. "That's an early call."

Dyn said the so-called distributed denial of service (DDoS) attack came in two waves, at first hitting its domain name system (DNS) platforms in the Asia Pacific, South America, Eastern Europe, and western United States regions.

But as it began to raise its defenses, the attack switched to direct intense traffic at its eastern US platform. It took about two hours to rebuff the attack.

Two hours later a second attack was launched, and it took Dyn about an hour to put that down.

The attack was magnified many times over by millions of "retries" of internet addresses by legitimate users and the machines involved in the attack.

That made it hard for Dyn to distinguish legitimate from attack traffic.

"We saw both attack and legitimate traffic coming from millions of IPs (internet providers) across all geographies," it said.

Dyn said it is working with other companies to strengthen their defenses.

"This attack has opened up an important conversation about internet security and volatility," Dyn executive vice president Scott Hilton said in a statement.

"Not only has it highlighted vulnerabilities in the security of 'Internet of Things' (IOT) devices that need to be addressed, but it has also sparked further dialogue in the internet infrastructure community about the future of the internet."