Disgruntled gamer 'likely' behind October US hacking: expert

November 16 2016

In October, a hacker used a powerful malware program known as Mirai to arness some 150,000 "Internet of Things" devices to overwhelm the systems of Dynamic Network Services Inc, which operates a key hub in the internet

The hacker who shut down large parts of the US internet last month was probably a disgruntled gamer, said an expert whose company closely monitored the attack Wednesday.

Dale Drew, chief security officer for Level 3 Communications, which mapped out how the October 21 attack took place, told a Congressional panel that the person had rented time on a botnet—a network of web-connected machines that can be manipulated with malware—to level the attack.

Using a powerful malware known as Mirai, the attacker harnessed some 150,000 "Internet of Things" (IoT) devices such as cameras, lightbulbs and appliances to overwhelm the systems of Dynamic Network Services Inc, or Dyn, which operates a key hub in the internet, according to Drew.

The so-called distributed denial of service attack jammed up traffic routing the Dyn's servers to major websites like Amazon, Twitter and Netflix for hours before the attack could be overwhelmed.

"We believe that in the case of Dyn, the relatively unsophisticated attacker sought to take offline a gaming site with which it had a personal grudge and rented time on the IoT botnet to accomplish this," he said.

Drew did not identify the gaming site but The Wall Street Journal, citing people familiar with the attack, said it was the PlayStation network.

At the time, there were worries that a foreign government might have been behind the attack.

Drew said the ability of hackers to make use of mundane home electronics to mount such an attack signalled a huge new risk in the global internet circuitry.

He said IoT devices often have easily hackable passwords, including hard-wired passwords that owners cannot change.

"IoT devices also are particularly attractive targets because users often

have little way to know when they have been compromised. Unlike a personal computer or phone, which has endpoint protection capabilities and the user is more likely to notice when it performs improperly, compromised IoT devices may go unnoticed for longer periods of time."

He noted that such devices are widespread around the world, including in areas with few cybersecurity protections, and that the October attack made use of "just a fraction" of those available. Mirai, he said, has infected nearly two million devices connected to the internet.

"The current lack of any security standards for IoT devices is certainly part of the problem that ought to be addressed."