Huge hack 'ugly sign of future' for internet threats

11 February 2014 By Dave Lee Technology reporter, BBC News

http://www.bbc.co.uk/news/technology-26136774

A massive attack that exploited a key vulnerability in the infrastructure of the internet is the "start of ugly things to come", it has been warned.

Online security specialists Cloudflare said it recorded the "biggest" attack of its kind on Monday.

Hackers used weaknesses in the Network Time Protocol (NTP), a system used to synchronise computer clocks, to flood servers with huge amounts of data.

The technique could potentially be used to force popular services offline.

Several experts had predicted that the NTP would be used for malicious purposes.

The target of this latest onslaught is unknown, but it was directed at servers in Europe, Cloudflare said.

Attackers used a well-known method to bring down a system known as Denial of Service (DoS) - in which huge amounts of data are forced on a target, causing it to fall over.

Cloudflare chief executive Matthew Prince said his firm had measured the "very big" attack at about 400 gigabits per second (Gbps), 100Gbps larger than an attack on anti-spam service Spamhaus last year.

Predicted attack

In a report published three months ago, Cloudflare warned that attacks on the NTP were on the horizon and gave details of how web hosts could best try to protect their customers.

NTP servers, of which there are thousands around the world, are designed to keep computers synchronised to the same time.

The fundamentals of the NTP began operating in 1985. While there have been changes to the system since then, it still operates in much the same way.

A computer needing to synchronise time with the NTP will send a small amount of data to make the request. The NTP will then reply by sending data back.

The vulnerability lies with two weaknesses. Firstly, the amount of data the NTP sends back is bigger than the amount it receives, meaning an attack is instantly amplified.

Secondly, the original computer's location can be "spoofed", tricking the NTP into sending the information back to somewhere else.

In this attack, it is likely that many machines were used to make requests to the NTP. Hackers spoofed their location so that the massive amounts of data from the NTP were diverted to a single target.

"Amplification attacks like that result in an attacker turning a small amount of bandwidth coming from a small number of machines into a massive traffic load hitting a victim from around the internet," Cloudfare explained in a blog outlining the vulnerability, posted last month.

'Ugly future'

The NTP is one of several protocols used within the infrastructure of the internet to keep things running smoothly.

Unfortunately, despite being vital components, most of these protocols were designed and implemented at a time when the prospect of malicious activity was not considered.

"A lot of these protocols are essential, but they're not secure," explained Prof Alan Woodward, an independent cyber-security consultant, who had also raised concerns over NTP last year.

"All you can really do is try and mitigate the denial of service attacks. There are technologies around to do it."

Most effective, Prof Woodward suggested, was technology that was able to spot when a large amount of data was heading for one destination - and shutting off the connection.

Cloudflare's Mr Prince said that while his firm had been able to mitigate the attack, it was a worrying sign for the future.

"Someone's got a big, new cannon," he tweeted. "Start of ugly things to come."