PHYS.ORG

Answers to your questions about massive cyberattack

March 29 2013, by Troy Wolverton

Here are some answers to questions about perhaps the biggest cyberattack ever, which recently targeted Spamhaus, an anti-spam group based in Geneva and London. It ended up slowing down or blocking access to numerous Internet sites.

QUESTION: Over what period did the attack occur?

ANSWER: It began on the evening of March 15 and appears to have ended March 26.

Q: What kind of attack was it?

A: It was a type of "distributed denial of service attack," or DDoS. In such attacks, Internet-connected computers are hijacked, usually to send bits of data to a particular company's servers. The aggregate data traffic overwhelms the company's servers, essentially making it impossible for other Internet users to connect to them.

Q: What was different about this attack?

A: Many past DDoS attacks involved "bonnets." Those are groups of consumer or business PCs that have been compromised and assembled into a network that sends requests directly to a targeted site, often without their owners' knowledge. In this case, though, the attack used misconfigured Domain Name System (DNS) servers. These are the computers that translate the Web and email addresses we type into their actual numerical Internet Protocol addresses.

The attackers sent to the misconfigured DNS servers requests for information that pretended to be from Spamhaus. Spamhaus was eventually overwhelmed by the traffic.

Q: Why did the attack affect sites other that Spamhaus?

A: Spamhaus turned to CloudFlare, a San Francisco-based Internet security company, for help. After CloudFlare got Spamhaus back online, the attackers turned their attention first to CloudFlare and then to the network operators upon which CloudFlare depends for bandwidth and the Internet exchanges through which data to CloudFlare flows. Traffic from the misconfigured DNS servers started to fill up those networks and exchanges. In some cases, that traffic from the cyberattack overwhelmed other, legitimate traffic flowing through those networks and exchanges.

Q: How big was the attack?

A: At the time that Spamhaus turned to CloudFlare, the attack was sending 10 gigabits per second of data to Spamhaus. At the peak of the attack, it was generating 300 gigabits per second of traffic.

Q: Who was affected by the attack?

A: The attack appears to have largely affected Internet users in Europe and some parts of Asia. It's not known precisely how many people or websites were affected.

Q: Who was behind the attack and why?

A: The perpetrators of the attack aren't yet known. Because they were able to mask their identities to the DNS servers, they could be hard to trace.

Q: What can be done to prevent future attacks?

A: Regular Internet users are basically powerless to prevent the type of attack that hit Spamhaus. They can, however, prevent their computers from being hijacked for botnet-style DDoS attacks by using antivirus software and keeping it up to date.

People who have their own Internet servers for their business or personal use can check to see if they are configured properly to prevent the DNS attack. The Open DNS Resolver Project at OpenResolverProject.org allows users to plug in their server's address to find out whether it has been configured properly.

(c)2013 San Jose Mercury News (San Jose, Calif.)
Distributed by MCT Information Services

Citation: Answers to your questions about massive cyberattack (2013, March 29) retrieved 19 April 2024 from https://phys.org/news/2013-03-massive-cyberattack.html