The Spamhaus attack – now for the aftershock

Joakim Sundberg, 2013-26-04

In retrospect it is not too surprising that the Spamhaus attack would provoke a response... and here it is. Today, Sven Olof Kamphuis was arrested in Barcelona by an operation orchestrated by Eurojust, The European Judicial Cooperation Unit. He had been pointed out as the man behind the Spamhaus attack late last month. Sven runs CyberBunker, the company that got their domains black listed by Spamhaus.

This, though, was not the reason he got arrested. He has also been identified as the unofficial spokesperson behind the group called STOPhaus that has been pointed out to be the group behind the attack. The group is connected to Russian and Chinese hacking groups and were mooted as possibly the originators of the attack.

As a result of the arrest of Sven a group identified themselves as freecb3rob – cb3rob being claimed as the nom de guerre of Sven - have posted a press release on pastebin threatening all government organisations complicit in believing that Sven was involved in the DDoS attack against Spamhaus. They demand that Sven is released, otherwise they will launch 'the biggest attack u humans have ever experienced' towards Internet infrastructure.

Their immediate focus is the Netherlands where Sven is supposed to be deported for further criminal processing. On Thursday, KLM, the national airline of The Netherlands , was hit by a DDoS attack that lasted for some time. The online check-in service was unavailable and suffered from several types of DoS attacks.

Today it was the turn of DigiD. DigiD is the national electronic identification service hosted by the Minister of Interior. According to a spokesperson no user information has been compromised in the attack and the attack has been mitigated by denying traffic from IP addresses outside NL.

So far everything is pointing towards this being a DDoS attack to make a statement and disrupt service. The real question is whether this group or groups can release an attack of the scale that would impact the Internet's infrastructure. So far we have seen traffic floods of ~300 Gbps using DNS reflection attacks.

We have definitely not seen the end of this operation if we should take freecb3rob by their word. For more information on DNS Reflection attacks reference my earlier blog post.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com