

www.availabilitydigest.com

# **Spamhaus Attacker Caught**

May 2013

A massive Distributed Denial of Service (DDoS) cyberattack was waged against the Dutch spam-filtering company, Spamhaus, for ten days during March of this year.<sup>1</sup> It is believed to be the largest DDoS attack in the history of the Internet. The alleged mastermind of the attack, Sven Olaf Kamphuis, 35, has now been arrested in Spain and has been extradited to The Netherlands. There he will stand trial under Dutch law for the criminal offense of launching a DDoS attack.

## The Attack

#### The Victim

Spamhaus is an anti-spam watchdog group that works alongside law enforcement agencies such as the FBI (the U.S. Federal Bureau of Investigation), email providers, and networks around the world.

Spamhaus provides a blacklist of IP addresses for servers that are determined by Spamhaus to host email spammers. The list is provided to ISPs, corporations, and spam-filtering vendors. The lists are typically used by these organizations to restrict incoming information from spamming sites.

It is estimated that 1.4 billion Internet users are protected by the Spamhaus blacklist. This means that 1.4 billion users cannot receive anything from a listed site.

#### The Attackers

CyberBunker, named for its headquarters in an old NATO five-story bunker, is a Dutch web site that claims it will host anything but child pornography and terrorism-related content. The CyberBunker web site was designated a spam site by Spamhaus and is on the Spamhaus blacklist. Understandably, the management of CyberBunker, headed by one Sven Olaf Kamphuis, was very unhappy with Spamhaus for blacklisting it.

In retaliation for this, a massive DDoS attack was launched against Spamhaus in an attempt to shut it down. A group calling itself Stophaus has claimed responsibility for the attack, calling their activities "Operation Stophaus." CyberBunker and Kamphuis have denied responsibility for the attack, but Internet forensics clearly point the finger at them both.

### The Attack

The DDoS attack against Spamhaus lasted from March 18 to March 28, 2013. The attack started out fairly small, driving about 10 gigabits per second (gbps) against the Spamhaus servers. Spamhaus

<sup>&</sup>lt;sup>1</sup> <u>History's Largest DDoS Attack?</u>, Availability Digest, April 2013. http://www.availabilitydigest.com/public\_articles/0804/spamhaus.pdf

maintains a distributed architecture through data centers in The Netherlands and Great Britain and easily weathered this storm.

The attack then escalated to 75 gbps, which matched the largest known DDoS attacks to date. Spamhaus enlisted the aid of CloudFare, a U.S.-based security firm to help it out. CloudFare spread the attack across many of its 23 data centers to filter out malicious traffic and deliver just legitimate traffic to Spamhaus.

In retaliation, CloudFare became included in the attack, and the malicious traffic increased to 300 gbps, a level never before seen in a DDoS attack. CloudFare was able to scrub even this level of traffic, and Spamhaus continued in business, albeit with some difficulty. Finally, on March 28<sup>th</sup>, the attacks stopped.

#### The Internet Vulnerability that Fueled the Attack

Classically, DDoS attacks are launched by *botnets*. Botnets are thousands of infected PCs (or in some cases, volunteered PCs) that will send traffic to a site upon command from a botnet control center. A typical PC botnet might be able to generate several gbps of malicious traffic.

To increase the scale of the attack, botnets are now emerging using infected servers. A large server can generate hundreds of times the traffic that a PC can deliver. With server botnets, malicious traffic measured in the tens of gbps can be generated. It is this sort of botnet that was used to attack on several occasions major U.S. banks by Islamist hactivists demanding that the offensive video, "Innocence of Muslims," be withdrawn from the Internet.<sup>2</sup> These attacks involved attack rates of 50 to 75 gbps.

How did the Spamhaus attackers achieve hundreds of gbps of attack data? They used a vulnerability in the Internet that has been known for years and that experts have warned may one day be used as a weapon. The method is called a reflected DNS attack. The internet is loaded with old DNS servers that will respond to any request to convert a URL to an IP address, not just to requests from their domains. These DNS servers are known as *open resolvers*.

A reflected DNS attack is quite simple. A DNS query to convert a URL to an IP address is sent to an open resolver with a spoofed sender IP address. The spoofed IP address is that of the site to be attacked. The result is that the response to the request is sent to the attacked site. The key to success of this method of attack is that a request message is about thirty bytes, but the response is more in the order of 3,000 bytes. Thus, there is about a hundred-to-one magnification factor. An attacker need only generate three gbps of URL requests to flood a site with 300 gbps of malicious traffic.

There has been an effort to get rid of open resolvers. Unfortunately, this is not high on the priority list of busy IP network administrators. There are currently 27 million open resolvers on the Internet, and their IP addresses have all been published.

# Sven Olaf Kamphuis

Dutch authorities were able to track the source of the Spamhaus attack to Spain and to Sven Olaf Kamphuis directly. Dutch judicial authorities issued a European warrant for the arrest of Kamphuis.

Spanish law enforcement arrested him at his home in Granollers, about 35 kilometers north of Barcelona, Spain. They confiscated computers, storage devices, and mobile phones from his home. Spanish police reported that Kamphuis had a van equipped with antennae to scan various frequencies. It was, in effect, a mobile command center from which Kamphuis could hack into networks from anywhere in the country.

<sup>&</sup>lt;sup>2</sup> Islamic Hactivists Attack U.S. Banks, Availability Digest; October 2012. http://www.availabilitydigest.com/public\_articles/0710/bank\_attacks.pdf

Kamphuis is the self-proclaimed spokesperson for the Stophaus attackers and describes himself on his Facebook page as the "Minister of Telecommunications and Foreign Affairs for the Cyberbunker Republic." It is unlikely that this will gain him diplomatic immunity.

He considers himself a campaigner for Internet freedom, and likens himself to Julian Assange, the WikiLeaks founder who publishes classified information and news leaks from anonymous sources.

Kamphuis describes Spamhaus as a company that wants "to get their way and shut people down. They do it all the time. If people do



Sven Olaf Kamphuis

not comply with their demands they just list the entire internet provider. That's what happened. It is not us but Spamhaus who's censoring of people they don't like and mafia tactics that are threatening freedom of the internet at the moment.

"Spamhaus itself is a more urgent danger. Pointing at websites and saying they want it shut down and then they get it shut down without any court order. That is a significantly larger threat to internet and freedom of speech and net neutrality than anything else."

### **The Prosecution**

Kamphuis was extradited to The Netherlands on Monday, May 6<sup>th</sup>. He appeared before a court in Rotterdam on May 8<sup>th</sup>. Upon recommendation by the Dutch Public Prosecution Service, the court ordered Kamphuis held for fourteen days as the investigation continues. At that time, the court will decide whether to hold him in detention for a longer period of time.

The investigation is being led by the Dutch High Tech Crime Team. Kamphuis presumably will be charged with launching a DDoS attack, a criminal offense under Dutch law.

Kamphuis continues to deny his involvement in the attack. He maintains that the attack was launched by Stophaus members in China and Russia.

### The Attacks Continue

These guys don't give up. After Kamphuis' extradition to The Netherlands, Dutch government web sites were hit with DDoS attacks, From May 7<sup>th</sup> to May 8<sup>th</sup>, its Rijksoverheld.nl and Government.nl web sites were rendered nearly unusable by malicious traffic directed at them.

Via a posting on Pastebin on Tuesday, May 7<sup>th</sup>, a group who said that they were supporters of Kamphuis claimed responsibility.

### Summary

DDoS attacks are on the rise.<sup>3</sup> They are easy to accomplish, and can do significant damage to a company's public-facing web sites. Companies must be prepared to undertake emergency procedures to mitigate such attacks. This is becoming a must-have in Business Continuity Plans.

One possible approach is to have contractual relations with a DDoS mitigation company. These companies monitor a site's traffic and can detect a DDoS attack shortly after it begins. They advise companies what steps to take to thwart it. If these steps are inadequate, the mitigation company can redirect all traffic to its scrubbing centers and can forward only legitimate traffic to the victim company.

<sup>&</sup>lt;sup>3</sup> <u>DDoS Attacks on the Rise</u>, *Availability Digest*, April 2012. <u>http://www.availabilitydigest.com/public\_articles/0804/2012\_ddos\_activity.pdf</u>

# Acknowledgements

Material for this article was taken from the following sources:

Dutch cyberattacks suspect arrested in Spain, USA Today; April 26, 2013.

Dutch suspect 'SK' arrested for Spamhaus cyber attack called internet's largest, The Verge; April 26, 2013.

Spamhaus attack: Dutchman SK arrested in Spain for 'biggest ever 'cyberattack,' Telegraph; April 27, 2013.

Spamhaus cyberattack suspect rolled around Spain in 'hacking van' command center, The Verge; April 29, 2013.

Spain arrests suspect in massive cyberattack, CNN; April 29, 2013.

Suspected Spamhaus Hacker Sent Home to Netherlands, Huffington Post; April 29, 2013.

Police Arrest Spamhaus cyber attack suspect, Computer Weekly; April 29, 2013.

Cyberattack Hits Dutch Gov't: DDoS Suspect Extradited, NewsFactor, May 8, 2013.

Spamhaus DDoS suspect extradited to the Netherlands, Computerworld, May 8, 2013.

Spamhaus DDoS suspect extradited, faces Dutch court, ZDNet, May 9, 2013.