Spamhaus BGPf Case Study at Schibsted Media Group

Using Spamhaus BGPf in a production environment

The Spamhaus Project, Geneva, Switzerland
http://www.spamhaus.org

Table of Contents

1 Executive Summary

In 2012, Spamhaus launched a new service to protect internet users from cyber threats and crime being committed through these threats by using so-called Trojan horses - the Spamhaus BGP feed (BGPf).

In the past year, Spamhaus was able to identify thousands of malicious server operated by cybercriminals, hosting botnet command-and-control services (C&Cs), used to instruct compromised machines, exfiltrate data and steal sensitive information from its victims (e.g. credit card or e-banking information).

In mid 2012, we were able to test the power of our newly launched services in a production environment. In this case study we will describe the customers environment and how Spamhaus BGPf helped our customer to mitigate threats by controlling connections to malicious infrastructure.

Introduction

Spamhaus BGPf

Spamhaus BGPf is a service operated by The Spamhaus Project, an international non profit organization whose mission is to track cyber threats, such as spam and botnet (malware) operations.
BGPf is an abbreviation for our BGP feed, aimed to protect networks from malicious sources such as spam, malware and botnet traffic. Unlike other services run by Spamhaus, BGPf provides protection on the network layer by announcing a list of IP addresses and network ranges which have been identified by Spamhaus as being involved in certain types of malicious activities.

Spamhaus BGPf currently offers three separate lists:

Community	Name	Description
65190:1000	Spamhaus DROP	Serves Spamhaus DROP list
65190:2000	Spamhaus EDROP	Serves Spamhaus extended DROP list
65190:3000	Spamhaus BGPCC	Serves Spamhaus Botnet C&C list

Each list contains a different set of IP addresses identified by Spamhaus as sources of malicious traffic.

Spamhaus DROP/ EDROP

DROP (Don't Route Or Peer) and EDROP (Extended DROP) are advisory "drop all traffic" lists, consisting of stolen or 'hijacked' netblocks as well as netblocks controlled entirely by criminals such as spammers, malware authors, botnet operators and rogue neworks. DROP and EDROP are a tiny subset of the SBL and are designed for use by firewalls and routing equipment.

EDROP is an extension of the DROP list that includes suballocated netblocks controlled by cyber criminals. EDROP is meant to be used in addition to the direct allocations on the DROP list.
When implemented at a network or ISP's core routers, DROP and EDROP will help protect the network's users from spamming, scanning, harvesting, DNS-hijacking and DDoS attacks originating from rogue netblocks.

Spamhaus BGPCC

The Spamhaus Botnet Command and Control (C&C) list is an advisory "drop all traffic" list consisting only of single IPv4 addresses. The servers on these listed IP addresses host botnet C&C nodes. C&C nodes are servers that control the individual malware-infected computers (bots) that together form a botnet. Bots regularly contact C&C nodes in order to transfer their stolen data to the botnet's owner, and to receive instructions on what they are to do next. Once a bot contacts a C&C node, it can receive instructions to send spam, host spammed web sites, attack other hosts on the internet (DDoS), provide name service (DNS) for the domains used in those attacks, etc.

When installed in a router's DENY table, the Botnet C&C list prevents any communication between that router and the IPs on the list. If the list is installed on all routers for a given network, it results in blocked communication between the botnet controllers and any bots on that network. In other words, the Botnet C&C list prevents loss of sensitive information that can be used in identity theft, and interrupts the ability of any bots on that network to send spam or be involved in criminal activity.

Usage

Both lists (DROP and EDROP) as well as BGPCC can be used in different ways to provide protection against malicious traffic on different layers:

Type	Available lists	Protection Layer
BGPf	DROP, EDROP, BGPCC	Network (TCP/IP)
RPZ	SBL, DBL, DROP, EDROP, BGPCC	DNS
RSYNC	ZEN, SBL, XBL, PBL, DBL, DROP, EDROP, BGPCC	Any*
DNSBL	ZEN, SBL, XBL, PBL, DBL, DROP, EDROP, BGPCC	E-mail (SMTP)

* The RSYNC service provides all Spamhaus lists as plain-text feed which can be in fact used in a variety of ways, such as loading the lists into a local DNS or firewall configuration, or importing them into custom applications.

The Trial

Schibsted Environment

Schibsted Media Group has a dedicated subsidiary called Schibsted IT, which is in charge of the local IT infrastructure in Norway, as well as being a large hosting provider for Schibsted's online services and web portals. Schibsted IT manages approximately 3,000 clients, mostly Desktop and Mobile systems as well as operating nearly 2,000 servers which are being used to host various online services and online portals.

Online attacks against Schibsted IT

In mid 2012, the Schibsted IT infrastructure was hit by a series of serious Distributed Denial of Service attacks (DDoS), obviously aimed at bringing down parts of Schibsted's network. The attacks lasted for several months and Schibsted IT had a hard time identifying the source of the cause and mitigating the attack.
Schibsted contacted several local IT security service providers asking for assistance in this. However, none of them were able to help Schibsted in their mitigation process.
Schibsted finally managed to track down the attacks, which were associated with infected computers within Schibsted's internal client network: the criminals had tried to exfiltrate data from inside Schibsted, and the DDoS attacks were launched by the attackers as distractions from the actual crime being committed.

Mitigation using Spamhaus BGPf

Schibsted decided to subscribe to Spamhaus BGPf and implemented all three lists (DROP, EDROP and the Botnet C&C list (BGPCC)) on their network. Instead of just blocking the prefixes announced by Spamhaus BGPf on the network layer, Schibsted "sinkholed" the rogue IPs to a separate server under their own control. This revealed several infected computers within Schibsted's internal network that were infected with different pieces of malware. By using the sinkhole techniques, Schibsted was able to identify 2-10 infected computers on their internal network on a weekly basis, most of which turned out to be infected with a variant of the famous ZeuS Trojan.
As soon as Schibsted implemented Spamhaus BGPf and began sinkholing the malicious (botnet) traffic, they reported that the DDoS attacks suddenly stopped. Since Schibsted began using BGPf, they have registered a substantial decrease in DDoS attacks.

Conclusions

By allowing malicious traffic to pass on a network, criminals are enabled in their mission to exfiltrate data from that network or the network's client's personal computers. This harms the integrity of a company, its brand and its customers, as well as allowing the possibility of criminal misuse of a company's resources.
The BGPf case study by Schibsted has clearly shown that by allowing malicious traffic, a network becomes a target for cyber criminal behaviour.
Spamhaus BGPf is a good way to mitigate these threats. By blocking and/or sinkholing malicious traffic and dropping incoming IP packets from networks operated or owned by cyber criminals, it is possible to deny the criminals their desired outcome.

Schibsted experience with BGPf

"Spamhaus BGPf is an excellent service, allowing us to mitigate cyber threats and to block malicious traffic in both directions. It enables us to identify and clean infected computers within our internal network quickly, and to prevent cyber criminals from stealing sensitive data from our internal network using Trojan horses. It helps us to ensure the confidentiality and integrity of our network and the services we provide."

- User experience from an IT Security representative of Schibsted IT

Annex

About Spamhaus

The Spamhaus Project is an international non-profit organization whose mission is to track the Internet's spam operations and sources, to provide dependable real-time anti-spam protection for Internet networks, to work with Law Enforcement Agencies to identify and pursue spam gangs worldwide, and to lobby governments for effective anti-spam legislation.
Founded in 1998, Spamhaus is based in Geneva, Switzerland and London, UK and is run by a dedicated team of 38 investigators and forensics specialists located in 10 countries.
The Spamhaus team works with Law Enforcement Cyber Crimes teams worldwide, assisting investigations into spam senders, phishing, botnets and malware operations, and compiling profiles, backgrounds and evidence on spam gangs and spam operations.

About Schibsted Media Group

Schibsted was founded in 1839 and is Scandinavia's leading Media Group and operating businesses in several European countries with more than 7'000 employees in 27 countries. Schibsted has its headquarter in Oslo, Norway. Schibsted owns the two biggest national newspapers in Norway, Aftenposten and Verdens Gang. Schibsted also operates newspapers and online portals outside Norway, for example in Sweden (Newspaper Aftonbladet) , in Switzerland (online portal tutti.ch) and several other European countries.