Report of Spamhaus incident 20140227

Background:
Resilans AB manages large blocks of IP space. This has been done by the same persons since the 90's in various constellations such as Sunet/KTHNOC and now Resilans. We acted as last resort for getting prefixes of IP addresses before RIPE NCC started to take this responsibility. Resilans has the direct authority over a number of /16 and /15 blocks. Normally only ISPs have such blocks, where the customer is assigned IP addresses which the ISP routes. Resilans is not an ISP and instead has a role more like RIPE NCC in regards to IP address delegations.

Most of these addresses are delegated in chunks of /24's to different entities such as commercial companies, municipalities, counties, government agencies and other organizations, and are used via many different ISP's and Autonomous Systems.

Spam, distribution of unsolicited emails, is a large problem on the Internet. One of the many attempts to mitigate the in-flood of spam is to not accept incoming emails from IP addresses from known spammers. This is highly effective, given that the lists of IP address is high quality. Spamhaus is a company that generates such lists.

The concept is good and useful, and it is a good thing that this service exists. When a prefix is used to send spam, intentionally or unintentionally due to lack of security or other reasons, this prefix should be visible via their databases and users should not receive emails from those prefixes.

When such a block occurs from Spamhaus, and this is related to prefixes delegated from Resilans IP address space, we are always alerted, and we always act upon these alerts by contacting the customer to take action, or by reclaiming the IP address space if the customer does not take action. This has happened on several occasions. Resilans policy for acceptable usage explicitly prohibits the use of the IP address space for sending spam.

We used to have a good working relationship with Spamhaus and have always abided by their policies regarding how to communicate with them and which action to take in order to resolve the issues.

But on 20140227 this service turned into a full scale attack on Swedish users. Spamhaus decided to block several large blocks of IP ranges, they placed the following ranges in their block lists:

192.36.0.0/16
192.71.0.0/16
193.183.96.0/19
194.68.0.0/19
194.71.0.0/16
194.103.0.0/19

and several more prefixes. Some of the users in these networks include:

Riksrevisionen (The Swedish National Audit)
Swedish Armed Forces

Swedish Nuclear Fuel and Waste Management Co, SKB
Karlstads Kommun (Karlstad municipality)
Boverket (The National Housing Board)
Swedish State Power Board (Vattenfall)
Telefonaktiebolaget LM Ericsson
Oskarshamns Kommun (Oskarshamns municipality)
Linkoping University
Luftfartsverket (The Civil Aviation Administration)
Lantmateriverket (National Land Survey)
County Administration of Gothenburg
Östhammars kommun (Östhammars municipality)
Länsstyrelsen i Norrbottens lan (County Board of County Norbotten)
Myndigheten for Samhällsskydd och Beredskap MSB (Authority for Civil Contingencies MSB)
Täby kommun (Täby municipality)
Akademiska sjukhuset Uppsala (Uppsala University Hospital)
Chalmers University of Technology
Umeå Universitet (Umeå University)
SUNET (Swedish University NETwork)
Stockholms Universitet, DSV (Stockholm University)
D-GIX Service network (NETNOD)
Royal Institute of Technology
DNS root name server i.root-servers.net
Karolinska Institutet
Saab AB
Försäkringskassan (Social Insurance Agency)
Statskontoret (State Treasury)
Posten (The Swedish postal service)
Stockholms läns landsting (Stockholm County Council)
Vårdguiden (Health Care Guide)
Strålsäkerhetsmyndigheten (the Radiation Safety Authority)
Örnsköldsviks Kommun (Örnsköldsvik municipality)
Naturvårdsverket (Environmental Protection Agency)
AUTONOMICA DNS-services
IKEA IT AB
Statens Livsmedelsverk (National Food Administration)
Dagens Nyheter (Newspaper)
Vägverket (Swedish Road Administration)
European Space Agency (ESA)
Volvo Information Technology
SAS
NasdaqOMX
Aftonbladet (Newspaper)
NORDUnet
Spotify Ltd
Resilans AB
ftp-archive on SUNET
Sveriges Riksbank (The Central Bank of Sweden)
Stadsledningskontoret (The Executive Office)
Statens Jordbruksverk (Board of Agriculture)

And hundreds of other customers. Almost all of them took no part in sending any spam, or was in any way involved in any operation related to spam. A handful of prefixes was used by a customer to send spam, and based on that action Spamhaus decided to block all of the above. The prefixes used for sending spam have been revoked from the customer since the event.

We find the action taken by Spamhaus inappropriate and their actions calls into question whether they have the knowledge needed to responsibly manage lists suited for wide usage on the Internet. We would strongly encourage ISP's and users not to use their services until the flaws in their procedures revealed by this incident are corrected.