SIP Security Alert

Just recently we’ve learnt of several automated attacks on IP based phone systems.

This is the rough sequence of events when an attack occurs:

- The robot sends a sip invite to the target IP address on the standard SIP port 5060 UDP (we do not know how it decides which addresses to attack in the first place).
- If it receives a SIP error response then it knows that it is dealing with a SIP agent. Beginning at 200 it repeatedly sends in SIP register invites using the extension number as the password. The two that we have seen, tried all extensions between 200 and 9999.
- If there are any extensions with SIP passwords the same as the extension number then the robot will register with the PBX and make a very short call (just a couple of seconds) to test connectivity.
- If the call is successful the robot disconnects.
- It returns and re-registers on Friday evening at about 18:00 local time and then it starts as many calls as your PBX will allow, all to the same premium rate number.

The two we’ve seen called numbers in Sierra Leone. The scam is that the owners of the robot also own the premium rate line so they are effectively siphoning money from you to them.

The two cases that we’ve actually investigated both burnt about £4500 in the course of about 24 hours of constant calling. In both cases the user/owner of the PBX was running one or more extensions with passwords set to the same value as the extension number.

This is a pretty serious problem but it is very easy to guard against provided you use passwords which are different to the extension number. Releases of SARK starting from V2.1.14 generate strong passwords for your extensions when you create them. You will also be OK if you use some secret password that isn’t the same as the extension number.

If you do have extensions with passwords the same as the extension then we would strongly recommend that you change them as soon as possible in order to survive any attacks you may receive.