Ghost Calls

Mike Johnstone - 2024-11-21 - Troubleshooting

# Ghost Calls

SIPvicious was created as an inventory tool for IT Admins to manage SIP devices evolving into a scammer tool used to probe for PBX vulnerabilities. Thankfully SIPvicious and its annoying ghost calls are easily dealt with with the strategies listed here.

Calls from phone numbers like “100” or “1000” with silence at pickup are the result of probes against your SIP port (5060). Almost all such calls use a tool called SIPvicious which silently attempts to audit your PBX or phone system for any vulnerability.

While the vast majority of SIPvicious ghost calls fail to get beyond just the initial probe, with a bit of perseverance they can be prevented altogether.

### How they work

SIPvicious sends an INVITE to scan your system SIP port 5060 looking for vulnerable PBX systems to hack and ultimately route calls through. While vulnerable PBX systems are the hackers intended targets, the same INVITE to an IP Phone (or VoIP Phone) generates the ghost call ringing. The ghost calls are therefore generally just an annoyance, and will not generate a financial loss.

### Suggested prevention strategies

- Blacklist: Higher-quality firewalls will allow you to blacklist the offending IP range and ultimate source of the ghost calls.
- Limiting 5060 access: If your firewall permits, deny all traffic to your voice-port 5060 except traffic from our pubic voice proxy – 103.55.116.0/24
- Port Forwarding: If you are port forwarding you will need to filter traffic over port 5060
- Changing handset port: As a last resort try changing your SIP port (5060) to an alternative such as 50600.

## Yealink

Yealink phones provisioned through our Device Provisioning have been configured to block IP Ghost calls, and SIP vicious style attacks. If you need to manually set configure your phone follow the two-step process below:

1. Download the latest firmware for your handset from Yealink
2. Upgrade Firmware: Settings | Upgrade >> Select and Upgrade Firmware
3. Allow IP Call: Features | General Information and it should be DISABLED. Click confirm to accept the change.
4. Accept Sip Trust Server Only: Account | Advanced, at the very bottom. It should be ENABLED. This makes the phone only accept invite requests from the server it's registering to.