How Secure is our Business Service?

Santiago Garcia - 2024-12-24 - Peering, Ports and IPs

How Secure is our Business Service?

All fraud attempts start with hackers probing for specific types of account vulnerability, such as the use of default passwords on known devices, no firewall filtering on SIP Peering / Trunking, unprotected access to port 80 et al. Once identified the hacker's goal is to route calls via the compromised account to the world’s war-torn despotic locales. Hackers have no interest in making local calls. Once the account has been compromised, they’ll sell access to the unsuspecting victim’s CPE to unscrupulous calling card operators or similar specializing in routes to the world's hotspots. Hence it can be months before the hacker cashes in on the compromise.

The most basic thing you can do is a strong password, upper & lower caps, numerals, and a wildcard like % or &. For example, hAv3@nic3day is many times harder to crack than “haveaniceday”. Locking down your router's port 80 and for IT people always use implement firewall rules to limit access to your SIP Ports (5060, 5061, 50600) to your SIP service providers.

While we constantly monitor suspicious calling patterns, it is ultimately the customer's responsibility to ensure the end user equipment is secure. We have no liability for financial loss caused by illegal access to customer's phone equipment.

How we block Fraud Attempts

When your CPE is compromised, the attacker connects what initially looks like legitimate calls through your equipment. While there are patterns to successful attacks, attacks are always well planned and mostly occur sometime after the initial compromise. On our side we have a number of strategies to mitigate fraud; blocking IP addressing from common hotspots, similarly blocking calls to high-risk destinations.

Since Snowden, we now know that governments and even vendors as their proxies are hacking. All before the myriad of specialist password cracking algorithms and probing tools.

What should you do to prevent it?

- **Registration:** The resolution from your side is usually as simple as changing or providing strong passwords. If your account has been blocked by us for a suspected fraud attempt, it is essential that your password is immediately changed.
- **SIP Peering:** Administrators must limit all access to their WAN IP including most importantly SIP ports 5060 and port 80 to known service providers (such as us) and

system admins.

What happens after we have blocked your account?

- We will notify you by email of the international toll block on your account.
- Immediately the account will have been prevented from making overseas calls. As soon as you have reset the password, or hardened your firewall, we will re-enable the account to allow overseas calling.
- See also **Ghost calling.**

Occasionally staff will in error misdial the leading prefix, which our systems identify as a potential threat (e.g. Somalia is +252). We are generally quick to identify misdialled prefixes and after speaking directly with account holders will quickly unblock the account. Most customers are happy to put up with this minor inconvenience for the comfort of knowing we are actively monitoring call fraud attempts.