redsense
INTELLIGENCE OPERATIONS

VoIP Ecosystems: A Deep Dive

SUMMARY

The below methods can be used for several different types of malicious activities from call center support scams to just generic vishing campaigns. However, these attacks depend on providers not understanding their security postures and overall infrastructure and ways it can be used for abuse. The other is just purely on the ability for the attackers to convince the end users to click links, call numbers or provide information.

Voice over Internet Protocol (VoIP), also called IP telephony, is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the Internet, rather than via the public switched telephone network (PSTN), also known as plain old telephone service (POTS).

TYPES OF PREMIUM NUMBERS

1. Domestic Premium Numbers are the telephone numbers restricted to their origin. This aids in supplying access to all domestic numbers within a particular country or region for inbound calls to generate micro funds for businesses. Premium rate phone numbers are used to provide services with added value. The tariffs used are higher than usual and the amounts paid are sent to the service provider as payment. In-country promotion of domestic numbers makes it easier for market segmentation and targeting of specific services.
2. International Premium Numbers are a micropayment tool to bill as services. The numbers in this category would be compensated on a connected call and often can have fees based on the duration of the call time. These international numbers being used asl payment solutions are accessible from anywhere an international call can be made and can be used for a diverse number of services such as TV shows or service hotlines such as credit cards, or emergency assistance programs, or anything that would be considered acceptable by the local telephone providers to allow on their networks.
3. SMS Premium Numbers are great ways to build new revenue streams. This allows a provider or business to earn on every SMS received across the globe on SMS International Premium Rate Numbers. These can be used and a are an exceptionally good method for Contests, Voting and Polling.

SELLERS

Legal sellers: Those who have the authority to use these types of premium numbers and services. These would be the original target markets for the service providers or third parties.

Criminal sellers: Criminals who hack into routers or VoIP servers to get VoIP account data among other types of data to be used later or sold. They also can be part of a group of what is called initial access brokers, these are the actors who break into networks, prove they have access to the network and sell that access to the highest bidder.

RedSense has tracked multiple actors using this ecosystem to propagate malicious activity of various sorts. Numerous call centers operating in the AJP region purchase these accesses in order to service their clients. One such scam is the Bazar Call methodology used by numerous high tier threat actors to create an initial access vector inside otherwise secure corporate networks. This access generally comes in the form of a remote administration tool installed under the guise of helping the victim to attain a refund or resolve a technical issue.

By following the activities of these ground-level ecosystems, RedSense is often able to correlate sales, methods and actors to far more consequential operations, such as the BAZARCALL phenomena. All of these ecosystems are interconnected at various levels, and disruption of the malicious supply chain can result in a disproportionately large impact further upstream. Securing your own VoIP systems is critical, in order avoid finding your phone numbers associated with criminal activity.