Marshall Eddy

CS331-001

Vincent Skimmer

12 September 2016

Telephones and Telephony Technologies

Telephony is the field of technology involving the development, application, and deployment of telecommunication services for the purpose of electronic transmission of voice, fax, or data, between distant parties (Wikipedia). The most common attacks through telephony mediums are called Telephony Denial of Service, which is more commonly referred to as TDoS.

The TDoS consists in disabling the telephone system of a target entity. They can do this by saturating a phone number from the outside, it is very easy to disable, in a just a few minutes, all of the incoming and outgoing calls (itsecurity).

TDoS attacks are very similar to denial of service attacks (DoS). The attacker must have access to several communication channels or several SIP accounts (usually hacked). Then the attacker uses automated calling machines simultaneously and repeatedly calling one or several of the victim’s phone numbers. All communication channels of the target then become rapidly engaged. The affected business cannot receive or make phone calls.

The attack only ceases when the attacker decides to stop, thus allowing the the attacker to demand a ransom to stop the attack, essentially the same thing as ransom-ware, but with telephony medians. Also, the effects of the attack may extend to rendering the whole of the unified messaging system useless in just a few minutes.

TDoS attacks can be difficult to detect because the attacker typically changes the caller ID on every call, making it quite difficult for service providers to even detect. Unless these attacks can be quickly traced back to an originating carrier that typically does not generate many calls to the contact center, they are very difficult to decipher between them and legitimate phone calls.

They also typically move through multiple service providers, making them time consuming to trace back to the source (krebs). Since these attacks can prevent both incoming and/or outgoing calls from being made, the most common targets of these attackers are government offices and emergency service that are very reliant on the use of a phone line.

An example of a specific technology related to telephony attacks is WarVOX. WarVOX is a free, open-source VOIP-based war dialing tool for exploring, classifying, and auditing phone systems. WarVOX processes audio from each call by using signal processing techniques and without the need of modems. WarVOX uses VoIP providers over the internet instead of modems used by other war dialers. It compares the pauses between words to identify numbers using particular voicemail systems. WarVOX was merged into the Metasploit project in 2011. The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

Telephone attacks can be performed remotely to access the telephone system program. This would allow them to potentially eavesdrop and record any conversion they are connected to. This would is probably utilized more so in a government aspect, could be for spying on other governments, or maybe even their own citizens. This would be on a much larger scale and implement multiple attacks on different telephone programs. This is helpful to attackers and frightening for the targets, as it is like having a wire tap, or ‘bug’, without having any sort of physical wire being connected, making it much harder to detect.

References

<http://krebsonsecurity.com/2013/04/dhs-warns-of-tdos-extortion-attacks-on-public-emergency-networks/#more-19472>

<https://en.wikipedia.org/wiki/Telephony>

<http://itsecurity.telelink.com/tdos-attacks/>

<http://www.bugsweep.com/system.html>