RSN Security Advisory – September 2020

SOCIAL ENGINEERING HACK DEMONSTRATES REQUIREMENT FOR VOIP THREAT INTELLIGENCE ANALYTICS

Condor Labs is isolating and recording large numbers of gangs preying on remote workforces and corporate VPNs through voice-phishing or vishing attacks. Vishing attacker focus predominantly involves financial institutions and crypto currency exchanges, telecom and mobile companies, SSO providers, enterprises, private individuals and public platforms such as social media sites and code-sharing sites.

These attacks, harnessing a combination of vishing and social engineering are more efficient, dangerous, and ubiquitous than previously seen. Attack activity is becoming so disruptive it has gained attention from the U.S. government who has issued both a warning and advice on how to thwart them.

Social engineering is the act of tricking someone into divulging information or taking action, usually through technology. It is a massive problem in the Cyber Security world and is one of the oldest forms of attack resulting in trillions of dollars of monetary loss. The idea behind social engineering is to take advantage of a potential victim's natural tendencies and emotional reactions.

To access a computer network, the typical hacker might look for a software vulnerability. A social engineer, though, could pose as a technical support person to trick an employee into divulging their login credentials. The fraudster is hoping to appeal to the employee's desire to help a colleague and, perhaps, act first and think later.

On July 22, 2020, Twitter reported 130 high-profile customer accounts were compromised causing worldwide concern. Many of the accounts were government staff and well-known celebrities. The attacker was found to be a teenager in Florida who collected ransom amounting to nearly US$121,000 in bitcoins.

Lab staff attack analysis found great interest in the hacker's discovery process. The hacker used a one-two punch on its victims through voice technology and preying on social engineering via human susceptibility. They obtained stolen usernames, passwords and two-factor authentication PIN codes through a fake page resembling VPN log-ins originating from the victim's corporate IT department. Fake customer calls into Twitter customer service and other social engineering methods convinced customer service agents to reset account holder's passwords. A straightforward attack vector that wasn't very sophisticated, but people lost money, and were embarrassed with potential for extended legal ramifications.

How this is done? A typical corporate user logs into their account with their username and password, and then a one-time PIN is issued to their cell phone. In this case, the victim was directed to a realistic hacker fake web page (phish page) where real users provided actual credentials and one-time-password to the hacker. The hacker would then simultaneously enter the same information into to the real corporate VPN and the victim to mask awareness of the hack.

Why execute this twitter hack? The attacks appear were intended for long-term access and short-term profit. Once the hackers completed the fraudulent help-desk call, they attempt to maintain access for several weeks. Their plan is to sell valuable privileged account access to other members of account takeover gangs, either to steal crypto currency or for bragging rights.

These voice and twitter hacks highlight the need for corporations to implement VoIP Threat Intelligence Analytics to proactively identify and shut down these types of malicious hackers.

Condor Labs' partner RedShift Networks delivers this powerful VoIP Threat Intelligence Analytics to prevent exploit by clearly reporting:

- Identify who is calling?
- Where are they calling from?
- What phone number are they calling from?
- Have they called one customer service number or multiple customer service agents?
- What type of phone are they calling from?
- Are they calling from the US or from an international number?
- And what type of attack are they conducting?
- Are they calling multiples times?
- Block these hackers when they are deemed to be fraudulent!!

REDSHIFT
NETWORKS

VoIP Threat Intelligence Analytics allows the enterprise to get a thorough multi-layer security picture of all voice communications inside and outside their network. This includes identifying employees to flag anomalous or strange behavior that could point to a possible attack or hacker.

RedShift Network's UCTM technology sits inside the production corporate voice network and delivers unprecedented visibility of all voice communications. The RedShift UCTM technology offers IT and compliance staff detailed information and stores voice real-time network information for current and future forensics for compliance and legal requirements:

- PCAP files on each call flow within enterprise,
- User Agents used by every employee and caller,
- IP addresses of caller whether he be calling from a US number or from an international location,
- Call History of every call flow,
- Detailed Call Registration history
- Block or Alert on more than 40,000 VoIP/Video Threats and attacks, and
- SIP Botnet attackers, Robo callers or other types of attacks.