Research Inventy: International Journal of Engineering And Science
Vol.12, Issue 1 (January 2022), PP 48-51
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Cyber Security in Cloud Telecom Operations

Natarajan.R[#1]
[#]*Department of Unified Communications, Accenture solutions Private Limited, Chennai, India*

Abstract— *Shifting from being a necessity to a lifeline, the telecommunications industry is now part of the beating heart for nationwide communications as the world navigates times of disruption and uncertainty. Unfortunately, this makes it a key target for cybercriminals wishing to profit from the information held by an array of businesses. Whether it be through financially driven criminal activity or high-powered state-sponsored attacks, the information being targeted has the potential to bring companies to their knees. Looking beyond the financial gain, a successful attack could threaten businesses' external internet traffic and damage customer relationships.*

Keywords— *Cyber telecom, cyber security, Telecom Vulnerability, Cloud Cyber telecom.*

Date of Submission: 14-01-2022 Date of Acceptance: 28-01-2022

I. INTRODUCTION

This Paper speaks about various cyber-attacks in Cloud Telecom service providers Which affects the telecom operations in Cloud Environment.

II. TELECOM CHANNELS IN CLOUD SECURITY

One of the primary methods used by cyber threat actors when targeting telecoms is SIM swapping – the act of swapping the SIM number associated with a phone to the SIM card in the attacker's phone. This gives them access to the victim's traffic, including the valuable two-factor authentication tokens that individuals receive in form of text messages. Two-factor authentication processes are used to protect highly sensitive information, including online banking and email accounts, however this isn't the only data at risk. Access to these tokens can also give criminals admission to almost any other third-party that uses SMS based two-factor authentication. This access may come in the form of insider threats which are a key route taken by criminals to conduct SIM swapping attacks. Malicious employees, who take advantage of their access to sensitive company information can directly reassign phone numbers to the attacker's SIM card. All SMS-based two-factor authentication codes can then be sent to the attacker rather than the victim.

Web shells and remote desktop provider (RDP) solutions are also common ways for criminals to acquire and transfer unauthorised network access to telecoms providers. For example, in October 2020, research uncovered that username "true-knight" offered to sell RDP access to the network of a US telecommunications provider for 0.5 bitcoins, the equivalent of approximately $6,500 at the time.

Whilst financial data is a popular target, criminals can use personally identifiable information (PII) for a range of fraudulent purposes. Attackers are interested in acquiring sensitive data points relating to identity, including dates of birth and social security numbers. Once criminals have gained access to VPNs and other services, personal information can be sold in criminal forums to be exploited in fraud and targeted cyber attacks.

For example, research into criminal forums in December 2020, uncovered the activity of username "x_04x", who was auctioning off administrative and VPN accesses to a telecoms provider in Jordon and Saudi Arabia. The VPN accesses would also enable further entry to other remote services, such as SSH, FTP and Citrix. With a starting bid price of $2,000 and a 'buy now' price of $3,000, the monetary gain is evident.

Gaining access to personal contact details and credentials is often just the first step. Attackers can also contact victims via their now-exposed phone numbers or email addresses and use those other PII details to give themselves credibility as fake customer service representatives.

In contrast to independent cyber criminals, state-sponsored threat actors often seek access to telecommunications service providers by way of collecting signals intelligence (SIGINT) on their customers, in the form of phones and internet traffic. If a foreign intelligence agency wishes to listen in on phone calls or gain access to text messages of a particular person of interest, telecoms become the ideal gateway to the relevant information.

Using the acquired information, these groups can either monitor ongoing communications between people of interest, target victims through social engineering attacks to install malware on their devices or contact

targets directly for potential recruitment as human intelligence (HUMINT) sources. Government intelligence agencies can also absorb bulk PII into searchable databases for future queries for a variety of purposes, such as background checks and screenings of visa applicants and foreign travellers.

The headline hitting SolarWinds supply chain breaches, uncovered in December 2020, raised the prospect of widespread compromises within the US telecoms industry, as all the top 10 US telecommunications providers were SolarWinds customers. The National Telecommunications and Information Administration, which is part of the US Department of Commerce, was one of the federal government victims of this supply chain attack. Its compromise could imply more specific interest in the targeting of the US telecommunications industry.

III. TELECOM RISK

For individual businesses and employees, one of the best defences against SIM swapping attempts is to use a mobile authenticator app. These apps will generate the two-factor authentication token locally on a phone and thereby eliminate dependence on the service provider, which is more vulnerable to attack. Other precautions, such as end-to-end encryption, can mitigate the risks of exposure to state-sponsored SIGINT collection via compromised internet service providers.

Insider threat programmes are a crucial way of monitoring for, and stopping, malicious insiders. Companies should implement strategies to identify vulnerabilities that could jeopardise the security of sensitive information. By minimising the access given to certain stores of data, businesses can detect and prevent insider attacks.

There are also many precautions that can be taken by telecoms organisations to protect both their own sensitive information, as well as that of their customers. Alongside advanced threat detection, companies should prioritise threat intelligence coverage of state-sponsored cyber espionage since the attacks of foreign intelligence services are more challenging for security teams to detect.

On top of internal preparations, external threat intelligence can also help security teams identify and validate emerging cyber threats targeting their organisations before they evolve into attacks. This proactive threat detection enables teams to react faster to threats and take measures necessary to ensure the security of their organisation's network and digital assets.

Ongoing monitoring of underground forums is one way that telecoms can detect potential threats early, as criminals quite often mention companies by name. This would allow them to investigate and uncover insider threats before any harmful action can be taken. Telecoms providers can benefit from a comprehensive external threat intelligence solution, equipping them with the necessary tools to face the wave of rapidly evolving cyber attacks that threaten their employees, end users, partners, and overall reputation.

Telecommunications is not an industry that can afford to take cybersecurity lightly. With the responsibility of protecting not only their own data but that of their customers, organisations must show dedication towards the deployment of necessary protections as they continue to face persistent threats.

IV. 5G CLOUD TELECOM RISK

Telecom Service Provider has determined that 5G implementation will introduce vulnerabilities in the following critical areas:

- **Supply Chain**: The 5G supply chain is susceptible to the malicious or unintentional introduction of risks like malicious software and hardware, counterfeit components, and poor designs, manufacturing processes, and maintenance procedures.
- **Deployment**: 5G will use more information and communication technology (ICT) components than previous generations of wireless networks. Improperly deployed, configured, or managed 5G equipment and networks may be vulnerable to disruption and manipulation.
- **Network Security**: 5G builds upon previous generations of wireless networks and is currently being integrated with 4G LTE networks that contain some legacy vulnerabilities, such as Distributed Denial of Service attacks and SS7/Diameter challenges. These vulnerabilities may affect 5G equipment and networks even with additional security enhancements.
- **Competition and Choice**: Despite the development of standards that encourage interoperability, some companies are building proprietary interfaces into their technologies, which limits customers' choices to use other equipment. Lack of interoperability with other technologies and services limits the ability of trusted ICT companies to compete in the 5G market.

To address these critical challenges, CISA and S&T are advocating that government and industry work collaboratively to maximize 5G's benefits and promote its security and resilience.

- **Encouraging continued trusted development of 5G technologies, services and products** — National investment in research and development (R&D), economic incentives for manufacturing, and buying

trusted components (or using economic deterrents for purchasing and installing untrusted components), will increase trusted production and lower the risks of malicious untrusted technologies.

- **Encouraging continued trusted development of the next generations of communications technologies**—5G technologies and standards will build upon themselves over time and security enhancements will continue. This development will occur in individual companies and in standards-making bodies as markets for new services take shape. However, the United States can encourage and invest in such development, potentially decreasing the influence of adversarial nations and decreasing U.S. reliance on untrusted technologies.
- **Promoting international standards and processes that are open, transparent, and consensus-driven and do not place trusted ICT companies at a disadvantage**—Global standards bodies, including the International Telecommunication Union and the 3rd Generation Partnership Project, should promote currently-adopted 5G-related standards and collaborate on their development.
- **Limiting the use of 5G equipment with known or suspected vulnerabilities**—The federal government is limiting the adoption of 5G equipment that may contain vulnerabilities through Section 889 of the 2019 National Defense Authorization Act, The Federal Acquisition Supply Chain Security Act, and Executive Order 13873 "Securing the Information and Communications Technology and Services Supply Chain."
- **Engaging with the private sector on risk identification and mitigation efforts**—The private sector can help mitigate 5G vulnerabilities and provide insight on where government support or intervention is needed, such as the development of best practices, convening industry and government partners, and prohibiting untrusted equipment will help secure 5G technologies and networks.
- **Ensuring robust security capabilities for 5G applications and services**—The federal government and industry partners will take a prevention-focused approach developing security capabilities that protect not only the 5G infrastructure, but also the applications and services that utilize it. Secure 5G applications and services will likely mitigate the risk of malware being transported across protected devices and defend against unauthorized command and control from exploited connected devices. Secure infrastructure will also guard against these threats and mitigate lateral threat movement within the 5G network.

Telecom Service Providers will soon be launching "Secure and Resilient Mobile Network Infrastructure" (SRMNI) R&D projects to support Subscribers number-one priority: securing the wireless communications supply chain .

"The benefits and new capabilities that will be realized through the adoption of 5G will provide tremendous value to the nation, its people and its economy. Telecom Service Providers are engaging with its private-sector R&D partners to develop solutions that will make 5G adoption secure, ensuring that its promised benefits will be realized at all levels of government and by all private entities."

Telecom Cloud Security project, which has an overarching goal to ensure secure and resilient critical mobile communications networks, will create innovative approaches and technologies to protect legacy, current and 5G mobile network communications, services and equipment against risks identified in the Current Scenario.

Telecom Service Provider 5G network security focus will develop innovative approaches that will leverage 5G to define methods and approaches to achieve:

- Flexible 5G security architecture tailored for a government environment
- Government-controlled security policy
- End-to-end security for the mobile device to the core
- Approaches to implement interoperable secure unclassified voice across Federal Government departments and agencies

V. CONCLUSIONS

This paper concludes the cyber security solutions provided by Service providers to the subscribers and also this paper speaks about 5G Cloud Telecom operations and its cyber attacks to the subscribers.
Cyber security in Telecom operations is required to keep the vulnerabilities under control in Cloud Telecom.

ACKNOWLEDGMENT

Special Acknowledgement to Cloud Telecom service providers such as AWS,Google,Vmware,Rehat

REFERENCES

[1]. White paper on Cloud Cyber security by US Telecom Department, Jan 2021
[2]. White paper on Cloud Telecom by US Telecom Department, Jan 2020
[3]. White paper on Cloud Telecom Cyber security by British Telecom, June 2019

Natarajan.R#. "Cyber Security in Cloud Telecom Operations." *International Journal of Engineering and Science*, vol. 12, no. 1, 2022, pp. 48-51.