SECURE YOUR EVERYTHING™

TELECOMMUNICATIONS:
AN INDUSTRY UNDER HEAVY SIEGE

Introduction

According to research, for the past seven years, hackers have penetrated mobile operations with a dozen Telecommunication Services Providers (TSPs). These hacks gained complete control of their networks, exposing call data records of hundreds of millions of customers.[1] However, the researchers noted that the geolocation data, call logs, and text message records were stolen from less than a 100 targeted high-profile victims with positions in government and the military.

This discovery raises a serious question. Is this the work of nation-state hacking groups seeking intelligence on foreign operations? Researchers say "yes."

Governments are exploiting telecoms to engage in covert surveillance.[2] Geopolitical unrest is helping to fuel cyber espionage, using illicit computer access to steal confidential information. These widely publicized hacks have damaged reputations and breeched data confidentiality and privacy agreements with customers. Fears of election meddling are stoking fears so high that US officials issued warnings that nation-states are attempting to manipulate public opinion ahead of the 2020 elections.[3]

With so much at stake, how are such intrusions possible?

Attackers are using tried-and-true hacking methods. They've exploited known vulnerabilities, including malware hidden in a Microsoft file or an exposed public server on the internet to gain access.[4] The malware then searches computers on the same network and floods the compromised network with login attempts until the hackers locate the crown jewels - caller data records database. Additionally, attackers spoofed personal social media pages of privileged users within a targeted organization to unleash malware on their computers. Elevated access privileges have been used to penetrate the network.[5]

In this paper, we'll explore the modern telecommunication service provider (TSP), and help define what steps can be taken to better secure the internal infrastructure and safeguard customers. With TSPs dynamic landscape, the ongoing pressures to transform digitally, and the anticipated rollout of 5G mobile networks, advanced cyber security will become even more essential.

[1] "A hacker assault left mobile carriers open to network shutdown," by Alfred Ng, c|net, June 25, 2019
[2] "Global Cyber Executive Briefing: Telecommunications," Deloitte.
[3] "U.S. Elections are Still Vulnerable to Foreign Hacking," by Tim Lau, Brennan Center for Justice, July 18, 2019
[4] "A hacker assault left mobile carriers open to network shutdown," by Alfred Ng, c|net, June 25, 2019
[5] "Global Cyber Executive Briefing: Telecommunications," Deloitte.

The modern telecommunications service provider

Rapidly advancing communications technologies and market pressures to digitize operations have altered today's TSP into a new breed of business beyond basic telecom services. The new formula blends consumer and business communication services to speed growth and increase revenues. A single provider can offer consumers analog and digital landline and mobile, broadband internet, and media entertainment. For businesses, telecoms offer managed services focused on communication, security, data center, network, among others.

AT&T Inc. is the world's largest telecommunications company with recent annual revenue soaring to $183 billion.[6] It's not only the largest provider of mobile and landline telephone services, but as the parent company of WarnerMedia, AT&T is now one of the largest media and entertainment companies in the world. Its diversification is exemplified by its own description as a "modern media company whose mission is to inspire human progress through the power of communication and entertainment."[7]

Why target telecommunications?

For cyber criminals, the answer is easy, "Why not?"

Telecom's vast, critical infrastructure of interconnected networks, its ever-growing portfolio of apps and services, and huge stockpiles of sensitive customer data, make it an attractive and lucrative target for cyberattackers. A growing attack surface and vectors make telecom organizations vulnerable to security attacks. One source estimates that the telco services market that includes fixed-network and mobile services will reach nearly $1.46 trillion in 2020.[8]

Beeline, a Russian telecommunications company with clients in Russia, Asia, and Australia, admitted the breach of data of 8.7 million customers. The actual security breach took place in 2017, but the data was only recently sold and shared online.[9]

[6] For 12 months ending June 30, 2019, "AT&T Revenue 2006-2019," Macrotrends

[7] Source: https://about.att.com/pages/company_profile

[8] "How blockchain technology is disrupting the telco industry: A guide," by Dr. William H Nguyen, Telecoms, December 11, 2019

[9] "Data breach at Russian ISP impacts 8.7 million customers," by Catalin Cimpanu, ZDNet, October 7, 2019

Mobile threat landscape

The GSM Association (GSMA), an organization representing more 1000 mobile operators and other companies in the broader mobile ecosystem, cited the mobile threat landscape will increase as companies introduce new services and technologies.[10] "Continued underinvestment in appropriate technology, processes, and people has resulted in numerous threats being realized against operators." GSMA cited these threats impacting mobile telecommunications networks in 2018:[11]

- **Supply Chain**—suppliers manage their own security controls, applying what they believe is necessary
- **Privacy and Data Protection**—failing to understand different jurisdictions and their different controls can result in mishandling of data and regulatory fines
- **Signalling**—aging protocols are not easily replaced so compensating control need to be adopted
- **Cloud**—adopting cloud technologies presents risk within the supply chain and deployments as operators outsource service management
- **Internet of Things**—consumer-driven threat with masses of insecure IoT devices and enterprise-driven threats where critical services are managed via IoT devices
- **Human**—risk with insider threats (intentional attacks and unintentional mistakes)
- **Device**—network-attached vulnerable devices introduce numerous threats

[10] "Mobile Telecommunications Security Threat Landscape," GSM Association, January 2019

[11] Ibid.

Domain Name System hacks

TSPs maintain large Domain Name System (DNS) server farms required to translate domain names to IP addresses so browsers can load internet resources. DNS is highly vulnerable to cyberattacks such as with DNSpionage. Cyber criminals stole email and other login credentials from government and private sector organizations in Lebanon and the United Arab Emirates by hijacking DNS servers and redirecting the stolen information to an attacker-controlled internet address.[12] Following these reports, the U.S. Department of Homeland Security issued an emergency directive ordering U.S. federal civilian agencies to take these four actions:[13]

ACTION 1 → Audit DNS Records

ACTION 2 → Change DNS Account Passwords

ACTION 3 → Add Multi-Factor Authentication to DNS Accounts

ACTION 4 → Monitor Certificate Transparency Logs

[12] "A Deep Dive on the Recent Widespread DNS Hijacking Attacks," by Brian Krebs, Krebs on Security, February 19, 2019

[13] "Emergency Directive 19-01: Mitigate DNS Infrastructure Tampering," cyber.dhs.gov, January 22, 2019

5G: Business as usual or a major disruption?

The 5G mobile communication standard is driven by the 3rd Generation Partnership Project (3GPP), a group of telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDI, TTA, TTC). Along with the adoption of new capabilities with each new generation, 3GPP ensures each new generation offers backwards and forwards compatibility where possible.

5G's new multi-services capabilities, including faster peaks speeds, lower latency, greater reliability, and broad unused spectrum are expected to fuel current and new use cases, including:[15]

5G stands for fifth-generation cellular wireless, and the initial standards for it were set at the end of 2017. But a standard doesn't mean that all 5G will work the same—or that we even know what applications 5G will enable. There will be slow but responsive 5G, and fast 5G with limited coverage.[14]

- **Improved broadband**—offers spectrum in bands not used for commercial broadband traffic
- **Autonomous vehicles**—allows vehicle-to-vehicle communications to help avoid accidents and save lives
- **Public safety and infrastructure**—enables cities and municipalities to operate more efficiently
- **Healthcare**—ultra-reliable, low latency communications (URLLC) with 5G can open up new healthcare solutions such as telemedicine, remote recovery, AR-based physical therapy, and more precise surgery
- **IoT**—faster speeds and low latencies will see IoT powered by communications among sensors and smart devices (mMTC), requiring fewer resources

[14] "What is 5G? Here's everything you need to know," by Christian de Looper, Digital Trends, August 20, 2019
[15] "The Evolution of Security in 5G," 5G Americas Whitepaper, October 2018

It's clear 5G networks are slowly making their debut, with China and South Korea leading the way. China currently claims the world's largest 5G network with commercial services available in 50 cities.[17] To support this initial effort, 12,000 5G base stations have been activated according to Xinhua, China's state news agency. The 5G data plans begin at 128 yuan (USD $18) for 30 GB of data per month, servicing some 850 million smartphone users.[18]

5G Americas membership organization consists of wireless carriers, network equipment providers, device manufacturers, and other providers that support the advancement of 5G. The group has stipulated that for 5G to live up to its full potential it must be delivered securely.[16]

However, although 5G is creating massive buzz around the world, security researchers are finding design flaws and vulnerabilities in the 5G protocol. Researchers from Purdue University and the University of Iowa say there are 11 new design flaws that could potentially expose a user's location, downgrade service to previous data networks, run up wireless bills, or even track calls, text, or web browsing.[19]

Of particular interest to mobile phone carriers (and their customers) is a possible security flaw where a cyber attacker could mount "'replay attacks' to run up a target's mobile bill by repeatedly sending the same message or command."[21] The researchers cited vague wording in the 5G standard that could lead to weak implementation by carriers.

In an official statement, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) said 5G implementation will "introduce vulnerabilities related to supply chains, deployment, network security, and the loss of competition and trusted options."[22]

"Since many security features from 4G and 3G have been adopted to 5G, there is a high chance that vulnerabilities in previous generations are likely inherited to 5G too.[20]

[16] "The Evolution of Security in 5G," 5G Americas Whitepaper, October 2018
[17] "China just launched the world's largest 5G Network," by Sherisse Pham, CNN Business, November 1, 2019
[18] Ibid.
[19] "As 5g Rolls Out, Troubling New Security Flaws Emerge," by Lily May Newman, Wired, November 11, 2019
[20] Ibid.
[21] Ibid.
[22] "Overview of Risks Introduced by 5G Adoption in the United States," Cybersecurity and Infrastructure Security Agency, July 31, 2019

Advanced cyber security protects telecoms

While telecommunication service providers' vast infrastructures offer stiff cyber security challenges, there are strategies that can be taken to help safeguard an organization's operations, its employees, and its customers. As discussed above, telcos and other service providers as well as virtually all industries are vulnerable to cyber attacks. Research firm Cybersecurity Ventures estimates that the damages from cybercrime may cost the world $6 trillion a year by 2021, double from the $3 trillion in 2015.[24]

"Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputation harm."

— Steve Morgan, founder and Editor-in-Chief, Cybersecurity Ventures.[23]

Consolidated security architecture

Like many organizations rushing to digitize their businesses, telecoms, too, are incorporating cloud, SaaS, mobility, and IoT technologies as well as having to integrate a large number of third-party suppliers and partners into their infrastructure. TSPs have been involved in mega merger and acquisition deals. In 2018, AT&T and Time Warner struck a merger agreement worth $85.4 billion. Sprint and T-Mobile, the third and fourth largest carriers in the U.S. are involved in a proposed $26.5 billion-dollar merger.

The rapid expansion of technologies and market flux reinforces a popular saying that your security is only as strong as your weakest link. This, in part, might be a big reason why telcos are a big target, but there are other reasons.

Like other industries, TSPs have relied on point solutions to protect each new attack vector and component. However, the net result has been a patchwork of security devices, opening up gaps for opportunistic attackers. Plus, a point solution approach impacts your security team where they must monitor numerous user interfaces to find and respond to an overwhelming number of diverse security alerts.

[23] "Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021," PR Newswire, Cybersecurity Ventures, December 13, 2018

[24] "SA suffers as cybercrime rises globally," by Mariam Isa, fin24, January 6, 2020

The option is to employ a robust consolidated security architecture that can secure threat vector as well as provide other data-loss-prevention and forensic-analysis tools. This strategy allows telecoms to cover all customer-facing technologies and infrastructure components whether on-site, SaaS, cloud, and mobile environments. All vectors can then be monitored and managed through a single interface.

A consolidated security architecture for all threat vectors has other advantages. Cyber security components talk to each other to offer more effective protection against 5th generation multi-vector attacks. IT staff can monitor the whole environment all at once. Streamlined monitoring raises security effectiveness while it lowers the burden on and the cost of security staffing, especially when having to manage multiple cyber security vendors.

Prevention

Many cyber security products and services use a minimum five-minute window to detect in-progress malware attacks. However, today's polymorphic malware can avoid detection systems and spread rapidly throughout a network. Cyber security that relies on detection can fail to prevent malware. This can explain telecoms struggle to prevent data breaches.

There are viable options. Cyber security solutions can now offer proactive attack prevention to stop malware threats before penetrating a network. Prevention, instead of detection, also simplifies and reduces the workloads required by security and IT teams. Advanced cyber prevention also uses artificial intelligence (AI) and/or machine learning (ML) and behavioral analysis. Small cyber security point products are unlikely to have access to the sufficient threat intelligence needed to adequately train their AI/ML engines for effective threat prevention.

Conclusion

With digital-first initiatives in full swing, telecommunication organizations can expect even further complexity with their IT systems. Implementing a consolidated security architecture that extends advanced threat prevention to all areas of the telecom environment streamlines cyber security operations, which greatly increases security effectiveness. Telecom IT is complex. However, with the right strategy, risks and costs can be brought under control.

To learn more how the Check Point Infinity security architecture helps consolidate your cyber security and solve your critical issues, visit us at https://www.checkpoint.com/architecture/infinity/ or contact your Check Point representative.

A case in point

"Check Point enables us to capture firewall, IPS, and anti-malware in a single platform. When you look at the kind of visibility Check Point gives you, it's way ahead of the platforms from all the other vendors." – *Kennedy Kimani, Head of Internal IT, MTN Nigeria.*

This major, international telecommunications services provider protects critical infrastructure with a consolidated security approach. Read the details here.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com

© 2020 Check Point Software Technologies Ltd. All rights reserved.