TELECOMMUNICATIONS – NETWORK SECURITY

ROOT LEVEL RESOURCES

The telecommunications sector is one of the top targets of government-backed groups who seek to attack critical infrastructure frameworks of other governments. By compromising a company in the sector, attackers can gain access to its customer database and use it for espionage and sabotage. Such actions have negative consequences for national security in the political, economic, social, information, environmental and other realms.

Main challenges to network security in the telecommunications sector:

Telecommunication services are highly reliant on various interconnected means of communication such as router, communicators, servers. As a result, telecommunications security problems can spring from various sources and can quickly spread throughout the network.

BGP hijacking

The threat is the potential of redirecting network traffic of an autonomous system individual prefixes (IP-address pools) through equipment.

Vulnerable routers

Outdated equipment can create new areas of vulnerability. This can decrease service quality and lead to increases in malicious traffic.

2G/3G/4G

Security gaps in mobile networks can lead to attackers bypassing traffication, using communication services at the expense of other customers, intercepting SMS messages, listening in on conversations, changing service terms, bypassing operator's restrictions, unabling the unsafe mode, or otherwise compromising subscriber communication. In addition, attackers can get access to the bank accounts of subscribers.

5G

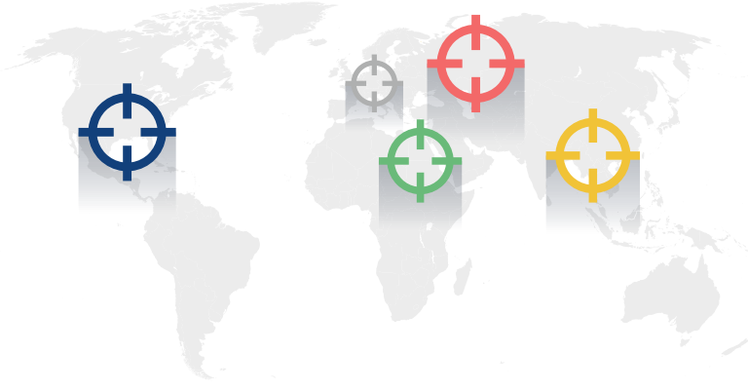
(new driver of threats)

The transition to 5G technologies (which is expected to be completed by 2021) creates new opportunities for attackers and will become the main target of leading attackers. This means individual vendors may become targets of attacks. A plethora of anonymous studies on the vulnerabilities of certain technological solutions are expected to be produced.

All this can exacerbate the scale of the threat. Vehicles and medical life-support systems can be targeted.

Government-backed groups that threaten the sector:

Over the past few years, information security experts have identified a number of new state-sponsored groups. Many of them have been carrying out attacks on the sector for a long time but managed to go unnoticed. Additionally, many of them employ similar tactics and have similar goals, which creates competition and makes the process of detecting them more difficult.



Group Name/ Activity Period	Geography of main attacks	Penetration Vector	Tools
APT 10 (China) *January 2012 – present time*	Europe; Asia-Pacific Region	Modified web-shell version	Poison Ivy RAT
WINNTI (China) *January 2017 – April 2019*	Asia-Pacific Region; Middle East and Africa; Russia and CIS	"Living off the land" - the use of legitimate local applications for malicious purposes such as to install Trojans	ShadowPad
MUDDY WATER (Iran) *September 2017 – present time*	Europe; Middle East and Africa; Russia and CIS	Attacks through LAN access of a mobile operator	Powerstats
THRIP (China) *January – June 2018*	Unspecified	"Living off the land" - the use of legitimate local applications for malicious purposes such as to install Trojans	PsExec, Mimikatz, WinSCP и LogMeIn
APT33 (aka Elfin, Magnallium) (Iran) *June 2016 – December 2018*	USA; Europe; Middle East and Africa	Rewriting MBR, partitions and files in the system with randomly generated data	Shamoon
CHAFER (aka APT39) (Iran) *July 2014 – present time*	Middle East and Africa; Asia-Pacific Region	Phishing, scanning of letters, use of stolen accounts	POWBAT, Antak, Asxpy
LAZARUS (North Korea) *March 2016 – November 2018*	USA; Europe; Asia-Pacific Region; Middle East and Africa; Russia and CIS	Targeted phishing, social networks, watering hole-type attacks	Ratankba, PowerRatankba, ClientRAT, ClientTraficForwarder (Proxy), AppleJeus, PowerTask, PowershellRAT, Banswift/BBSwift, RatankbaPOS, Mimikatz, Metaspoit, Dtrack, Rising Sun
LYCEUM (also known as HEXANE) *April 2018 – present time*	Middle East and Africa; Russia and CIS	Attacks through providers (Supply Chain), targeted phishing, selection of passwords, brute force	DanBot, Posh C2, PowerShell Empire

Security problems in the telecommunications sector, along with sabotage and espionage, are the primary reason behind the loss of personal data and customer financial information. This often means that the attacked telecommunication companies are held responsible (fined large amounts of money) for their inability to implement necessary safeguards and other measures to protect customer data, in accordance with the provisions of the GDPR (General Data Protection Regulation).

It is worth noting that most government-sponsored groups are in competition with each other and tend to reveal the tools and tactics used by their rivals online.

On the one hand, this helps expose criminals. On the other hand, it allows them to continuously improve their methods and hide more effectively in the future. Actions of state-funded groups are usually centrally planned at the strategic, tactical and operational levels. They are carried out in a closely-controlled way. As a result, it is increasingly difficult to identify attacks and attackers, and to bring them to justice.

Therefore, the main hope is that technology developers and network security providers can close old security gaps and avoid new ones, improving router safety, while reducing the risk of attacks in the telecommunications sector.

Sources:

ROOT LEVEL RESOURCES

1 Reports of Secureworks // URL: https://www.secureworks.com/

2 Reports of Dragos // URL: https://dragos.com/

3 Reports of Group-IB // URL: https://www.group-ib.ru/

4 Reports of Positive Technologies // URL: https://www.ptsecurity.com/ru-ru/