February 2023

GSMA
Mobile Telecommunications Security Landscape

This is a Whitepaper of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

About GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com.

www.facebook.com/gsma/
twitter.com/GSMA
www.youtube.com/gsma
www.linkedin.com/company/gsma/
www.instagram.com/gsmaonline/

Table of Contents

GSMA CTO Foreword

The mobile industry is providing critical national infrastructure in demanding times. Mobile coverage and usage gaps have been identified as prime areas for change. Recent significant geopolitical events underline the key role mobile telecoms plays during conflict by keeping civilians connected. Against this backdrop, maintaining and enhancing the security of mobile networks and devices is a vital activity. Given the challenge, we will succeed by working together to develop and implement security best practices.

This Mobile Telecommunications Security Landscape report describes some of the key security threats identified during 2022. Importantly, the report draws on both public sources and reports from within the GSMA security community. Please take the time to read this report and get involved in this team effort. Existing GSMA members can continue to contribute to our security work and are encouraged to apply GSMA security guidelines and recommendations within their businesses. Other interested stakeholders are welcome to get involved: they can do so by joining the GSMA, which will ensure access to a breadth of security advice and best practices.

Alex Sinclair - Chief Technology Officer, GSMA

GSMA Fraud and Security Group Chair

The inherent value of what we do with our mobile phones and the uses of the mobile network in every business sector across the world means that our industry is a big focus for attack.

Users of mobile technologies are targeted by a variety of actors – whether it be low-level fraud via phishing, smishing, or through social engineering against them or call centres. As our technology becomes more secure, the human is targeted because they are seen as the weakest link. We've seen businesses targeted in similar ways, including insider attacks. In our own industry, attackers can sometimes target 'low-hanging fruit' businesses in the supply chain or the way that operators technically interconnect their networks. For businesses, the threat of ransomware and data breach still looms large and there is clearly a lot of work to do to implement baseline security controls that raise the bar away from technical exposures that simply shouldn't be there.

The telecoms industry is not immune to internet threats and we've seen frauds that are 'cyberenabled' – that is they leverage IT vulnerabilities and systems, but with a telco-fraud objective. This has been increasing as attackers get a better understanding of mobile network technology and as the value of targets increases. Cyber and physical attacks against telco infrastructure and networks in conflict zones are also becoming the norm.

Whilst we spend much of our time working to secure future technology based on the experiences and knowledge we gain from previous attacks, we also carry the burden of legacy throughout. The mobile industry is somewhat unique in that we have a lot of technology and protocols still running which originate in the 1970s or before. They simply aren't designed for security, but they underpin a lot of what we do. In a similar fashion to the railways, network operators have to keep networks and services running whilst replacing the technology and making sure nothing breaks! Whilst our industry doesn't have Victorian railway arches to deal with, legacy is something that has become an Achilles heel when it comes to security. The unacceptable rise of private spyware such as Pegasus and others has taken advantage of this legacy, particularly in signalling protocols. Operators that don't deploy measures to monitor and protect signalling networks via the use of stateful firewalls will unfortunately continue to suffer the consequences.

As we continue to build technologies that blend and virtualise telecoms with the traditional IT world, increasing the attack surface, we'll also realise the security management benefits; a more mature ecosystem for threat intelligence sharing, including machine-readable and standardized mechanisms for rapid exchange of information. This will allow coordinated and quick responses to attacks, both preventatively and as they occur. As the reliance on the mobile network to economies grows, we'll see further threats that we'll need to counter accurately and quickly and we must continue to work to bridge the two worlds' experts and tools.

The threat information and actionable security intelligence that we share in our own industry and with others ultimately enables us to protect citizens across the world, whether it be using a mobile phone or driving a connected car.

David Rogers MBE - Chair, GSMA Fraud and Security Group & CEO, Copper Horse Ltd

1 Executive Summary

Welcome to the GSMA's fifth annual Mobile Telecommunications Security Landscape report, which builds on the previous reports to present an updated view of the evolving security threat landscape.

This year's report focuses on security threats that the GSMA has been tracking throughout 2022 both from public sources and from within the GSMA's membership. Items reported by the GSMA membership have been edited to anonymise the source of the intelligence and/or detailed attack techniques and are cited as 'GSMA Mobile Industry Intelligence'.

Key themes in the report include:

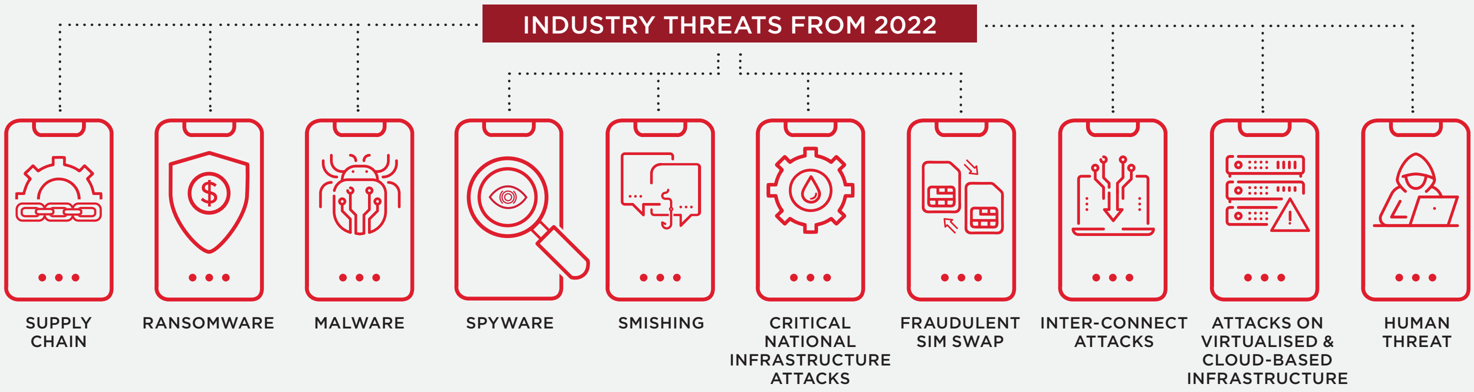
- → Infiltration. For example, obtaining some form of unauthorised system or data access.
- → Access exploitation. For example, using unauthorised access to perform a further exploitation, such as account access, lateral movement or privilege escalation.
- → Availability compromise. For example, some form of denial of service attack.

2022 saw the continuation of many previously observed security threats and this report therefore covers several topics that were included in previous reports, such as malware, ransomware and supply chains.

Additionally, this edition includes threats not previously covered, such as the human threat, critical national infrastructure attacks and spyware. Each section contains examples of the threat and additional information that further explains the threat.

The security topics discussed in this report are shown below.

Finally, the report presents the GSMA's approach to building mobile network security resilience and how the GSMA helps its members develop their security posture.



INDUSTRY THREATS FROM 2022

SUPPLY CHAIN

RANSOMWARE

MALWARE

SPYWARE

SMISHING

CRITICAL NATIONAL INFRASTRUCTURE ATTACKS

FRAUDULENT SIM SWAP

INTER-CONNECT ATTACKS

ATTACKS ON VIRTUALISED & CLOUD-BASED INFRASTRUCTURE

HUMAN THREAT

2 Introduction

Mobile networks are vital in providing and increasing mobile internet coverage and usage. Today[1], 96% of the world's population is covered by mobile broadband networks and more than half of the world is using the mobile internet. However, a usage gap remains[2]. Some 3.2 billion people live in areas covered by mobile broadband networks, but do not use the mobile internet.

Mobile services are being enhanced through increased deployment of 5G infrastructure[3] and to support a shift towards more flexible working. Changes in geopolitical dynamics mean that mobile infrastructure is subject to greater security risks arising from malicious interventions in supply chains and direct physical and electronic attacks on infrastructure. Given this backdrop, mobile network operators are safeguarding the confidentiality, integrity and availability of communications across the network by securing critical assets (hardware, software and data) and preventing unauthorised access or intrusion to any of the constituent nodes or links.

This fifth edition of the GSMA Mobile Telecommunications Security Landscape report builds on the previous reports to present an updated view of the evolving security threat landscape. This document aims to assist the mobile ecosystem by presenting key security topics through a lens of the security threat, while describing how the GSMA is helping the industry strengthen its security resilience.

This year's report focuses on reported security threats that the GSMA has been tracking throughout 2022 both from public sources and from within the GSMA's membership. Reported items from the GSMA membership have been edited to anonymise the source of the intelligence and/or detailed attack techniques and are cited as 'GSMA Mobile Industry Intelligence'. The aim is to evidence these threats in a way that can be shared in this public document and thereby illustrate the ongoing security challenges.

2022 has seen the continuation of many previously observed security threats and therefore this report covers several topics that were also included in previous reports, such as malware, ransomware and supply chains. Additionally, this edition covers threats not previously included, such as the human threat, critical national infrastructure attacks and spyware. Each section contains examples of the threat and additional information that further explains the threat. Note the list of topics is not exhaustive and any reader should make their own risk assessment based on their data and system assets, threat assessment and current/planned security posture.

[1] sdg-main-report-2022-web.pdf (gsma.com)

[2] The usage gap refers to people living in areas covered by a mobile broadband network, but not using mobile internet

[3] GSMA report '5G in Context, Q2 2022 Data-driven insight into areas influential to the development of 5G' (August 2022) identifies 738 million 5G connections (9% adoption) and forecast to reach 2.3 billion connections by the end of 2025 (26% adoption)

Mobile telecommunications network security operates within a wider ecosystem and there have been a range of complementary publications during 2022, including:

- Intel471's Commonly Observed Threats to Telecommunications Sector[4]
- Hardenstance's June 2022 report Defending Telecoms Against Nation State Cyber Threats[5]
- Connectwise's 2022 Cyberthreat Report for Managed Service Providers[6]
- European Union Agency for Cybersecurity (ENISA) Telecom Security Incidents 2021[7]
- ENISA's Threat Landscape 2022[8]
- IBM Security X-Force's Threat Intelligence Index 2022[9]
- CrowdStrike's Global Threat Report[10]

[4] https://intel471.com/resources/whitepapers/telecom-threats-2022
[5] Defending-Telecom-Operators-Against-Nation-State-Threats-FINAL.pdf (hardenstance.com)
[6] https://www.connectwise.com/resources/ebook-2022-msp-threat-report
[7] Telecom Security Incidents 2021 — ENISA (europa.eu)
[8] ENISA Threat Landscape 2022 — ENISA (europa.eu)
[9] https://www.ibm.com/reports/threat-intelligence/
[10] Report2022GTR.pdf (crowdstrike.com)

3 Ransomware

Ransomware is a type of remote malware-enabled cybercrime whereby the attacker initiates a successful compromise of a target system, then seeks to extort a ransom payment in return for restoring data, or not exposing or deleting data.

In 2022, new publications on this topic include:

- Microsoft blog and ebook on ransomware-as-a-service[11]
- ENISA's Threat Landscape for Ransomware Attacks[12]
- Hardenstance's White Paper: Adjusting to a New Era in Ransomware Risk[13]
- Copper Horse online analysis of Telecoms Industry Ransomware Victims[14]

Ransomware-related security threats reported in 2022:

- The US communications provider iBasis fell victim to a ransomware attack. The data subsequently published on the Darknet also contains references to Swiss telecommunications providers[15].
- A claim that Subex was hit by ransomware[16].
- Vodafone Portugal claimed to have been hit by ransomware (Lapsus$ group suspected)[17]
- The Lapsus$ group allegedly broke into NVIDIA's internal network and managed to steal sensitive data from hashed login credentials to trade secrets. The hackers wanted NVIDIA to remove the mining hash rate limiters on their RTX 3000-series graphics processing unit (GPU) as ransom[18].
- In January 2022, Okta detected an unsuccessful attempt to compromise the account of a customer support engineer working for a third-party provider[19].
- An incident involving an initial access broker (IAB) breaching a target and then selling that access on to a ransomware gang for use in their attack[20].
- The emergence of ransomware-as-a-service[21] (simplifying the technical aspects of a ransomware attack).

[11] https://www.microsoft.com/en-us/security/business/security-insider/anatomy-of-an-external-attack-surface/ransomware-as-a-service-the-new-face-of-industrialized-cybercrime/
[12] ENISA Threat Landscape for Ransomware Attacks — ENISA (europa.eu)
[13] White Paper: Adjusting to a New Era in Ransomware Risk | HardenStance
[14] https://copperhorse.co.uk/telecoms-industry-ransomware-victims/
[15] https://www.netzwoche.ch/news/2022-02-14/cyberangriff-auf-ibasis-schweizer-telkos-betroffen
[16] https://www.securitynewspaper.com/2022/01/10/ransomware-group-hacks-telecom-analytics-firm-subex-and-its-cybersecurity-subsidiary-sectrio/
[17] https://securityaffairs.co/wordpress/127799/cyber-crime/vodafone-portugal-massive-cyberattack.html
https://abcnews.go.com/International/wireStory/cyberattack-targets-vodafone-portugal-disrupts-services-82740716
[18] https://analyticsindiamag.com/lapsus-hack-leaves-nvidia-in-a-tight-spot/
[19] https://www.okta.com/blog/2022/03/updated-okta-statement-on-lapsus/
[20] https://news.sophos.com/en-us/2022/06/07/active-adversary-playbook-2022/
[21] https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

The wide reporting and severe nature of many of the attacks mean that ransomware continues to be a major security consideration for enterprises. A range of best practice countermeasures are emerging that maximise prevention and establish effective restoration from backups. The operational and financial impact of a successful ransomware attack, and therefore the security risk, can be significant. Together, the risk impact and likelihood of an attack can form the basis for a robust investment business case, leading to enhanced security controls and stronger defences. Ransomware insurance is a notable part of a risk transference strategy[22].

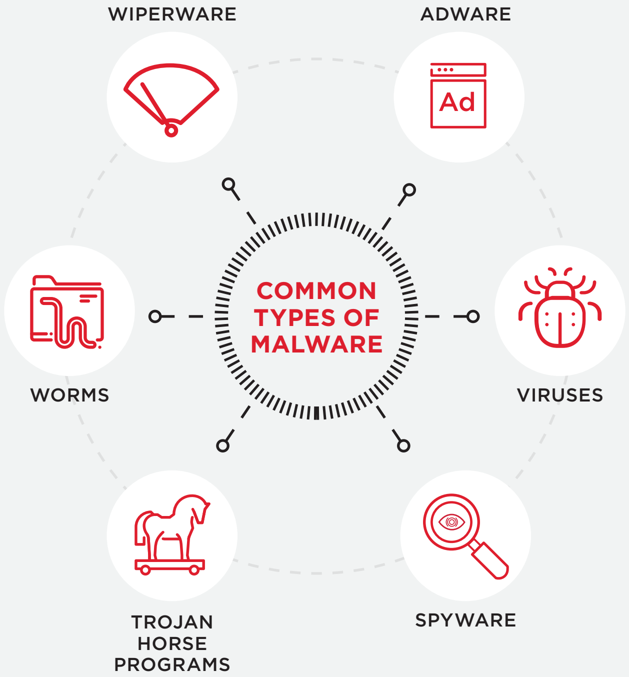
[22] Ransomware: An insurance market perspective (genevaassociation.org)

4 Malware

Malware' is short for 'malicious software' and is the generic term for any computer programme that is written with the intent of performing acts on a computing device (including mobile handsets) without the knowledge or permission of the owner or user of that device. Common types of malware are shown in the diagram.[23]

Malware-related security threats reported in 2022:

- US satellite communications provider Viasat was a victim of data wiper malware that affected routers and modems on the KA-SAT satellite broadband service impacting thousands of people in Ukraine and tens of thousands more across Europe[24].
- ThreatFabric described various forms of active malware, such as Hydra, Anatsa, Octo, Alien and Xenomorph. 'Dropper' applications for these malware families, which masquer aded as legitimate applications, were down loaded by Android users via Google Play[25].
- An Emotet malware spam campaign was reported to the GSMA by a mobile network operator from the Asia Pacific region[26].
- Chinese hackers launched a campaign using malware written in the Nim language and hidden in the SMS Bomber tool[27].
- A growing number of mobile VPN services in Europe led to the advent of new malware that sends SMS to international destinations[28].
- Avast has been tracking a widespread malware campaign consisting of TrojanSMS malware[29]



[23] malware - Glossary | CSRC (nist.gov)
[24] https://www.bleepingcomputer.com/news/security/viasat-confirms-satellite-modems-were-wiped-with-acidrain-malware/
[25] 2022 mobile threat landscape update — ThreatFabric
Malware wars: the attack of the droppers — ThreatFabric
[26] GSMA Mobile Industry Intelligence
[27] https://www.hackread.com/chinese-hackers-nim-language-malware-sms-bomber-tool/
[28] GSMA Mobile Industry Intelligence
[29] https://blog.avast.com/smsfactory-android-trojan

- There were reports[30] of abuse of compromised Android "platform certificates" potentially allowing an attacker to create seemingly approved malware permissions without user approval.

Malware, such as wiperware[31], can cause destructive data and operational outcomes that can have a more immediate and damaging impact than a more staged ransomware attack. Still, the defensive position for malware is similar to ransomware, so a combined and strategic security response can be effective.

[30] https://www.wired.com/story/android-platform-certificates-malware/

[31] Wiperware typically seeks to erase the hard drive or memory of the computing device it infects

5 Smishing

Smishing is phishing via SMS (short message service) where the aim is to try and trick users with messages that appear to be legitimate, such as alerts coming from banks.

Smishing-related security threats reported in 2022:

- Roaming Mantis SMS phishing was observed in Europe: researchers detected campaigns targeting Android and iPhone users in Germany and France with malicious apps and phishing pages. Roaming Mantis is a credential theft and malware distribution campaign that uses smishing to distribute malicious Android apps as standalone APK files outside the Google Play Store[32].
- Trend Micro highlighted a new mobile malware infection chain targeting both Android and iPhone devices. The chain is triggered by a smishing message that appears to be sent from a telecommunications company. The malware might have been designed to steal credentials associated with the membership websites of major Japanese telecommunication services[33].
- Members of a criminal group sent victims emails, text messages and other forms of mobile messaging, containing a phishing link (like Flubot) leading to a bogus banking website.[34]
- Cloud communications company Twilio said some of its customers' data was accessed by attackers who breached internal systems after stealing employee credentials in an SMS phishing attack[35].
- Verizon briefed that bad actors were sending spam text messages to some customers, which appear to come from the customers' own number. The text included information about a free gift with a phishing link at the end[36].

The smishing examples cited above and the related Flubot (see next section) attacks demonstrate the widespread and on-going prevalence of this attack type. Therefore, vigilance, consumer awareness and strengthened security defences (such as blocking measures based on identifiers of malicious messages) are required, combined with action by law enforcement agencies, such as that taken by the Metropolitan Police in the UK in response to an attack that may have impacted 200,000 people[37].

[32] https://www.bleepingcomputer.com/news/security/roaming-mantis-android-malware-campaign-sets-sights-on-europe/
[33] https://www.trendmicro.com/en_us/research/22/a/tianyspy-malware-uses-smishing-disguised-as-message-from-telco.html
[34] Phishing gang behind several million euros worth of losses busted in Belgium and the Netherlands | Europol (europa.eu)
[35] https://www.bleepingcomputer.com/news/security/twilio-discloses-data-breach-after-sms-phishing-attack-on-employees/
[36] https://www.theverge.com/2022/3/29/23001528/verizon-spam-texts-own-number-confirms-statement
[37] https://www.bbc.co.uk/news/uk-63736573

FluBot – Case Study

FluBot refers to a blended attack combining smishing and voicemail lures that can lead a victim to install banking malware through social engineering. It targets mobile users, with the greatest impact on Android devices where users have enabled sideloading of apps, but iPhones are not entirely immune. Once downloaded and installed on victim devices, the main objective of the FluBot malware is to obtain accessibility privileges/full access to the device. The malware then detects banking and cryptocurrency applications on the device and superimposes fake overlay windows when the applications are opened. This enables the malware to capture credentials and credit card details, which are relayed to a botnet command and control server. FluBot malware is also able to intercept messages and application notifications.

From a user-flow perspective, the infection method follows typical mobile malware infection patterns:

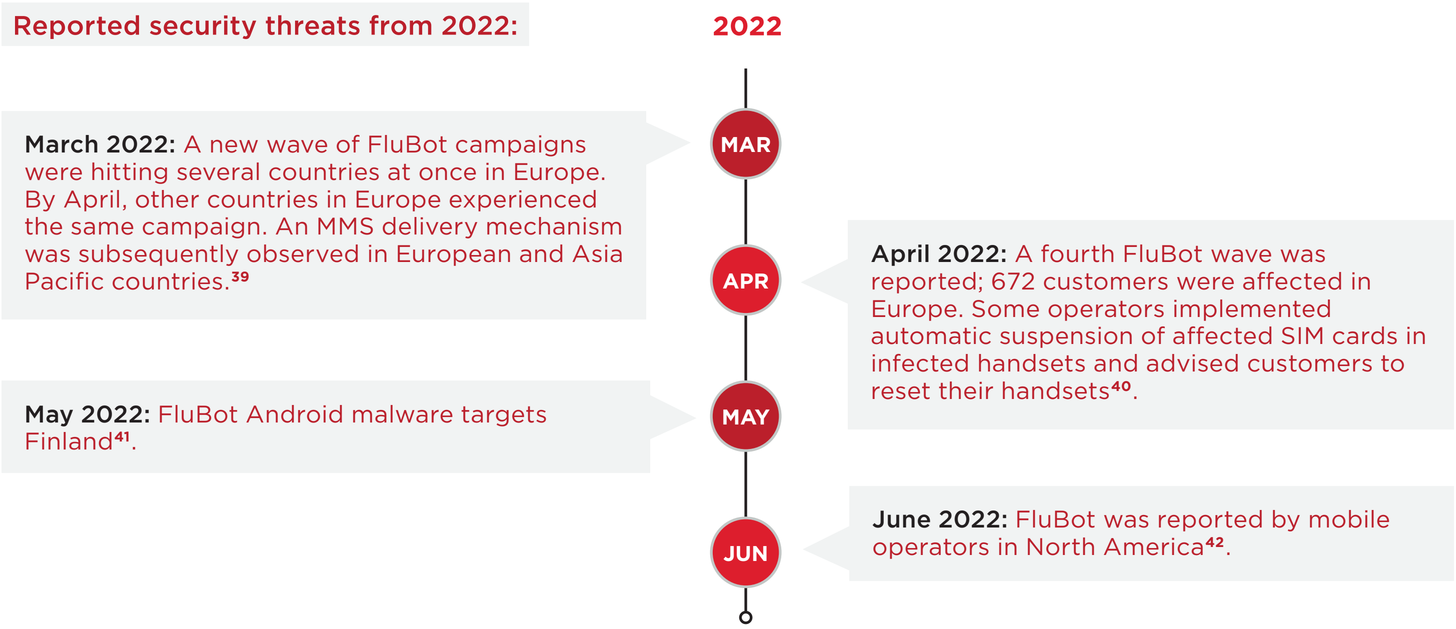
The victim receives a malicious SMS with a URL link.

The victim opens the URL link that downloads a malicious application.

The application is downloaded and installed, with the user being duped into sideloading the application and then approving application requests for privileges.

The malware gains access to the victim's contact list and sends the same malicious SMS to those contacts.

Adaptive Mobile has produced a timeline for FluBot that illustrates its evolution during 2022:[38]



Reported security threats from 2022:

2022

March 2022: A new wave of FluBot campaigns were hitting several countries at once in Europe. By April, other countries in Europe experienced the same campaign. An MMS delivery mechanism was subsequently observed in European and Asia Pacific countries.[39]

April 2022: A fourth FluBot wave was reported; 672 customers were affected in Europe. Some operators implemented automatic suspension of affected SIM cards in infected handsets and advised customers to reset their handsets[40].

May 2022: FluBot Android malware targets Finland[41].

June 2022: FluBot was reported by mobile operators in North America[42].

[38] What Is FluBot SMS Malware? How To Get Rid Of It? (adaptivemobile.com)
[39] GSMA Mobile Industry Intelligence
[40] GSMA Mobile Industry Intelligence
[41] https://www.bleepingcomputer.com/news/security/flubot-android-malware-targets-finland-in-new-sms-campaigns/
[42] GSMA Mobile Industry Intelligence

In June 2022, Europol reported successful countermeasures: "An international law enforcement operation involving 11 countries has resulted in the takedown of one of the fastest-spreading mobile malware to date. Known as FluBot, this Android malware has been spreading aggressively through SMS, stealing passwords, online banking details and other sensitive information from infected smartphones across the world. Its infrastructure was successfully disrupted earlier in May by the Dutch Police (Politie), rendering this strain of malware inactive." [43]

With the infrastructure take down, FluBot reports appear to have significantly reduced. Other smishing, copycat and 're-branded' attacks can be expected, so protective measures should be applied, including ensuring that devices are fully up-to-date with security updates where possible.

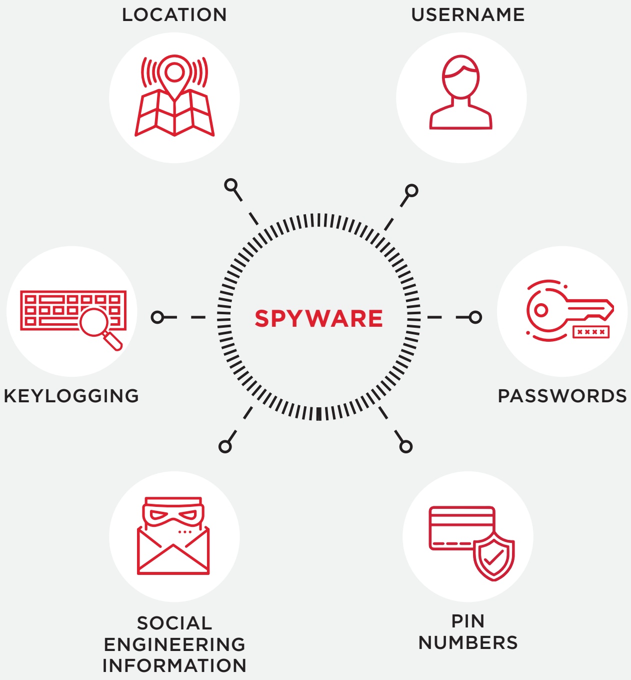
[43] https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

6 Spyware

Spyware[44] is a form of malware that is designed to steal confidential data from the computer or mobile device it is running on. Spyware can be used to access a range of personal information and other data (see graphic) to enable its author to gain unauthorised access to the services that these credentials are intended to protect. For example, mobile device spyware can steal location data, which then enables tracking of the device user.

Spyware-related security threats reported in 2022:

- There were allegations that Mitto, a company, operated a secret surveillance service that helped governments track mobile phones[45].
- The Spanish government has said the mobile phones of the prime minister, Pedro Sánchez, and the defence minister, Margarita Robles, were both infected with Pegasus spyware[46].
- Pegasus Spyware was allegedly used against Thailand’s Pro-Democracy Movement[47].
- The European Commission reportedly found evidence that employees’ phones had been compromised with spyware[48].
- Tykelab has been using several phone networks to send tens of thousands of “tracking packets”, targeting people in multiple countries including Libya, Nicaragua, Malaysia, Costa Rica, Iraq, Mali, Greece, Italy and Portugal[49].
- Hacking tools were reportedly used to spy on Apple and Android smartphones in Italy and Kazakhstan[50].



[44] https://www.cisa.gov/uscert/sites/default/files/publications/spywarehome_0905.pdf
[45] Mitto Tells Clients That Co-Founder Departed After Allegations of Phone Spying - Bloomberg
[46] https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware
[47] https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/
[48] https://www.reuters.com/technology/exclusive-eu-found-evidence-employee-phones-compromised-with-spyware-letter-2022-07-27/
[49] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[50] https://www.theguardian.com/technology/2022/jun/23/apple-and-android-phones-hacked-by-italian-spyware-says-google

The ongoing and apparent widespread use of spyware against civil society targets, journalists, government employees and human rights activists has prompted responses from governments in India, the US, the European Union and Israel. Defensive security measures for devices, such as vulnerability remediation and patching by original equipment manufacturers and operating system vendors, can also counter smishing, Flubot, ransomware and other malware. For network operators, close attention to SS7 signalling traffic, including the deployment and correct configuration of signalling firewalls, is crucial.

Spyware – Case Study

Incidents, such as those identified here and a number of previous reports, such as a blog post by Google[51] from 2017, have prompted a range of government interventions.

In the US, there was a House Intelligence Hearing on Combatting the Proliferation of Foreign Commercial Spyware[52]. One of a number of contributors, Carine Kanimba, spoke of her experience as an activist whose phone was targeted with the Pegasus spyware. Kanimba is the daughter of human rights activist Paul Rusesabagina[53]. The US Department of Commerce added the NSO Group, which developed the Pegasus spyware, to its entity list in late 2021[54]. In Europe, the EU has published it proposed regulation,[55] the European Media Freedom Act (EMFA) which, in part, aims to protect journalists from spyware and has convened its Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA) committee. The most recent PEGA meeting (5th December 2022) saw the presentation of the study:[56] The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware.

The United Nations General Assembly also published a report, The Right to Privacy in the Digital Age,[57] which covers the abuse of intrusive hacking tools, the role of encryption in ensuring the right to privacy and widespread monitoring of public spaces.

In India, the Supreme Court is considering whether there should be an investigation into the Government of India’s alleged use of Pegasus spyware on journalists, activists and public officials[58].

Much of the media coverage has been focused on the NSO Group’s Pegasus,[59] but this is not the only spyware in use; there are an increasing number of similar products. Google’s Threat Assessment Group tracks over 30 of these products.[60]

[51] https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html
[52] https://www.youtube.com/watch?v=H3oKYQiaIWA
[53] https://www.cnet.com/tech/services-and-software/threat-from-pegasus-spyware-still-looms-experts-testify/
[54] https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list
[55] https://digital-strategy.ec.europa.eu/en/library/european-media-freedom-act-proposal-regulation-and-recommendation & https://therecord.media/eu-moves-to-protect-journalists-from-spyware/
[56] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2022/12-05/Study_Pegasus_Legalframework_draft_5December_EN.pdf
[57] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf
[58] https://www.scobserver.in/cases/manohar-lal-sharma-prime-minister-pegasus-spyware-probe-case-background/
[59] https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know/
[60] https://blog.google/threat-analysis-group/googles-efforts-to-identify-and-counter-spyware/

7 Critical National Infrastructure Attacks

2022 has seen significant reporting of both alleged cyber and physical security attacks directly on critical national infrastructure, including telecommunications providers and on cable and power infrastructure.

Security threats to national infrastructure reported in 2022:

- In February, Vodafone Portugal suffered a major cyber attack that led to the loss of the entire network (i.e. all voice, data and messaging services) for several hours[61].
- Following a cyber attack, Optus responded to unauthorised access of current and former customers' information[62].
- The advanced persistent threat group GALLIUM was reported to have expanded its targeting across telecommunications, government and finance sectors with a new remote access trojan named PingPull. (PingPull has the capability to leverage three protocols (ICMP, HTTP(S) and raw TCP) for command and control[63].
- Slovak Telekom was hit by a large scale cyber attack[64].
- Adaptive Mobile Security released a whitepaper describing attacks over the mobile core network used as part of a hybrid warfare scenario[65].
- A compromise (possibly accidental) was reported on subsea communications cables connecting the Shetland Islands[66], whilst France is considering the adequacy of security of its submarine cables[67].
- A compromise was reported on an underwater power cable from Sweden to the Danish island of Bornholm.

Given the lengthy mean-time-to-repair for infrastructure compromises, resilient network design, with adequate redundancy and effective pre-emptive physical protection controls, is key to building effective defences.

[61] https://www.vodafone.pt/press-releases/2022/2/vodafone-portugal-alvo-de-ciberataque.html
[62] https://www.optus.com.au/content/dam/optus/documents/for-you/support/cyberattack/cyber_incident_letter_251022.pdf
[63] https://unit42.paloaltonetworks.com/pingpull-gallium/
[64] https://www.broadbandtvnews.com/2022/06/27/slovak-telekom-hit-by-cyberattack/
[65] https://blog.adaptivemobile.com/the-hunt-for-hiddenart
https://info.adaptivemobile.com/mobile-network-enabled-attacks-in-hybrid-warfare
[66] https://www.bbc.co.uk/news/uk-scotland-north-east-orkney-shetland-63326102
[67] https://www.politico.eu/article/france-tighten-subsea-cable-security-fear-sabotage-pipeline-gas-leak/

International Conflict – Case Study

Recent conflicts have involved a range of attacks and interventions against mobile networks, as part of a hybrid form of warfare. These attacks are among the more extreme and destructive security threats that exist.

As previously referenced, Techcrunch[68] reported a cyber attack on U.S. satellite communications provider Viasat, which triggered KA-SAT satellite service outages across central and eastern Europe, and was likely the result of destructive wiper malware. Sentinel Labs researchers believe it was the result of a new strain of wiper malware called "AcidRain" that was designed to remotely erase vulnerable modems and routers. Symantec reported[69] a new form of disk-wiping malware (Trojan.Killdisk) that was used in February 2022 and also found evidence of wiper attacks against machines in other countries. The businesses targeted included organisations in the financial, defence, aviation and IT sectors.

Sky reported[70] that fake mobile networks are being used to disrupt troops. False base stations have reportedly been attached to drones and located inside trucks to pick up the signals of nearby phones on the battlefield.

Adaptive Mobile Security, which claims to support the security of more than 2.1 billion subscribers worldwide, published a series of informative and comprehensive blogs covering the Ukraine conflict. The first blog[71] described the actions of the Ukrainian government and mobile operators in response to the invasion. These included release of additional spectrum, introduction of national roaming, maintaining service to customers running out of credit and suspension of all inbound roamers from Russia and Belarus. This latter action also had the benefit of reducing the interconnect attack surface. The second blog[72] addressed the impact of the war on the Ukrainian people, Russian invasion forces, the execution of war and preparation in advance of the war. The third blog[73] discussed the company's understanding of what 'cyber warfare' is (including "mobile-enabled effects") and a look forward to future developments in the 'mobile network battlefield'.

The Google Threat Analysis Group (TAG) reported[74] a growing number of threat actors using the war in Ukraine as a lure in phishing and malware campaigns and increased targeting of critical infrastructure entities, including oil and gas, telecommunications and manufacturing. TAG reported that APT28 or Fancy Bear was observed targeting users with a new variant of malware. The malware, distributed via email attachments within password protected zip files (ua_report.zip), is a .Net executable that steals cookies and saved passwords from Chrome, Edge and Firefox browsers. The data is then exfiltrated via email to a compromised email account.

Whilst building effective security resilience against advanced attacks by nation states is challenging, particularly in wartime, it is possible to create a strong set of defences[75] to provide broad and effective threat mitigation against a wide range of attack methods and threat actors. It is also important to consider how mobile networks can play a supporting role during any such conflict.

[68] https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper/
[69] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
[70] https://news.sky.com/story/ukraine-war-mobile-networks-being-weaponised-to-target-troops-on-both-sides-of-conflict-12577595
[71] https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-1
[72] https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-2
[73] https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-3
[74] https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/ 75 such as those outlined in the Building Mobile Resilience section of this report
[75] such as those outlined in the Building Mobile Resilience section of this report

8 Fraudulent SIM Swap

SIM swap is a legitimate service offered by mobile operators to allow customers to replace their existing SIM with a new one. A SIM swap may be required in the following circumstances:

- A SIM is lost, stolen or damaged;
- A different sized SIM is needed for a new device;
- The customer is porting out their number to a different network.

The ubiquitous SIM card is well understood by end users and remains a secure means for authenticating devices onto networks. Although the role of the SIM has not changed, the GSMA has defined a new way to load it into devices. Now the SIM may be securely downloaded into a 'secure element' that can be permanently embedded (the eSIM) inside any type of device.

While SIM swap is a necessary and useful service, it has provided an opportunity for fraudsters to obtain and utilise the replacement SIM card to gain access to users' financial and wider service accounts. Fraudsters seek to exploit the two-factor authentication commonly used by financial institutions to provide safe and secure services to customers. A common two-factor authentication method is to send a one-time passcode to the account holder's mobile number.

Fraudulent SIM and eSIM swaps exploit weaknesses in the mechanisms that mobile operators use to switch a mobile number over to a new SIM card.

Europol has produced an infographic on SIM swap[76]. Regulators in several countries are making moves to mandate stronger controls. For example, the regulator in Australia has introduced obligations for mobile operators to perform additional checks that apply when they carry out transactions such as SIM-swap requests[77].

SIM swap-related security threats reported in 2022:

- A persistent fraudster made over 50 separate calls to a mobile operator in Europe as a first step in an attempt to defraud its customers[78]. This is part of a wider trend where fraudsters carefully pick high value targets (e.g. some one with a very large cryptocurrency holding) and persist for dozens of calls over several days in their attempts to access their account and execute a SIM swap.
- Some cybercriminal forums even have an entire section dedicated to SIM swapping services. For example, in a high-profile Russian language cybercriminal forum, a user indicated they were interested in conducting SIM swapping attacks against "high-value targets" that have accounts with four named US-based telecommunications companies[79].

[76] https://www.europol.europa.eu/cms/sites/default/files/documents/sim_swapping.pdf
[77] https://www.acma.gov.au/articles/2022-06/new-id-check-anti-scam-rules-apply-today
[78] GSMA Mobile Industry Intelligence
[79] https://www.digitalshadows.com/blog-and-research/exploring-sim-swapping-services-on-cybercriminal-forums/

- Police in Spain reportedly dismantled a SIM swapping ring that drained bank accounts[80]
- The US Federal Bureau of Investigation (FBI) said that Americans lost more than US$68 million to attacks involving fraudulent SIM swaps in 2021, a number that has been exponentially increasing since 2018 when the agency first began tracking this threat[81].
- In 2022, a fraudulent SIM swap service was being openly advertised.[82]
- Customers are able to apply for and provision an eSIM online, for either prepaid or postpaid plans. A small number of bad actors exploit this ability to open or takeover accounts, either on postpaid by using stolen identities, social engineering or on prepaid using stolen credit card details. If successful, the fraudsters then start to conduct interna tional revenue share fraud (IRSF) while roaming. The fraud is more lucrative on postpaid accounts as they have the potential to generate a greater volume of traffic before detection[83].
- Other network operators have seen account takeover leading to a subsequent eSIM swap that later allows the attacker to compromise two factor authentication. This has been observed in Europe, Africa and Asia-Pacific[84].

The GSMA's Fraud Manual contains advice on countering fraudulent SIM swapping. Advice includes having an equal level of customer validation for new and existing customers, education and training of sales/dealer staff, multi-factor authentication and to consider implementing GSMA Mobile Connect[85] in order to authenticate users.

[80] https://arstechnica.com/information-technology/2022/02/police-in-spain-dismantle-a-sim-swapping-ring-that-drained-bank-accounts/

[81] https://therecord.media/fbi-68-million-lost-to-sim-swapping-attacks-in-2021/

[82] https://commsrisk.com/the-sim-swap-fraud-service-with-5-star-reviews/

[83] GSMA Mobile Industry Intelligence

[84] GSMA Mobile Industry Intelligence

[85] GSMA | Mobile Connect - Identity

A New Zealand Perspective – Case Study

Fraudulent SIM swaps and porting fraud are slightly different techniques employed by fraudsters to achieve the same outcome - gaining control of their intended victim's mobile phone number.

Mobile operators in New Zealand came together to develop a multifactor authentication solution to prevent unauthorised porting of a mobile number between them. A text message generated by a porting request needs an affirmative response for the port to complete. If the owner or account holder in possession of the number did not initiate or authorise the request, they are alerted by this message and encouraged to call their provider and bank to secure their accounts.

After implementation, the multifactor authentication solution saw an overnight halt in porting fraud. This pushed fraudsters back towards fraudulent SIM swaps. To counter this, some mobile operators restrict SIM swaps to in-store only meaning a fraudster needs to attempt an in-person transaction requiring ID which they are less likely to attempt or be successful with. However, there has been an increase in the number of high-quality counterfeit drivers' licences, with these being presented in store by fraudsters as a way around this. Nonetheless, the number of fraudulent SIM swaps is still significantly lower than the number of porting frauds previously seen.

9 Interconnect Attacks

The ecosystem supporting the provision of roaming and interconnect services is large, diverse and has complex interactions. Compromised interconnect services have the potential to expose customer data within signalling, user data traffic and the intermediaries associated with interconnection and roaming services. The actors involved range from MNOs and MVNOs to transit carriers, GRX/IPX providers, firewall management providers, roaming hubs, roaming VAS providers and messaging aggregators.

Traditionally, the interconnect traffic between mobile operators relied on the underlying signalling protocols for effective and secure operation and the inherent trust model that assumed that only those entities that need signalling access actually had it. For many years, this assumption has not been correct and operators need to recognise that attacks can come through their signalling network and their connections to other operators and partners.

The industry has developed a range of enablers to respond to this threat through the use of signalling firewalls, message filtering and blocking capabilities, security cooperation and intelligence/best practice sharing. However, signalling and interconnect remains an important and ongoing threat area that requires monitoring: when signalling is compromised, the integrity, confidentiality and availability of many services is at risk.

In 2022, the US agencies, the Cybersecurity & Infrastructure Security Agency (CISA), the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI), together with international cyber authorities, issued a cyber security advisory to protect managed service providers and customers.[86] Hardenstance's June 2022 report Defending Telecoms Against Nation State Cyber Threats[87] includes a section on the protection of interworking interfaces in telecoms.

Interconnect-related security threats reported in 2022:

- Syniverse 'May 21' incident relating to inter-operator roaming data and SMS traffic[88].
- T-Mobile's systems were subject to a criminal cyber attack that compromised the data of millions of customers[89].

[86] CISA, NSA, FBI and International Cyber Authorities Issue Cybersecurity Advisory to Protect Managed Service Providers (MSP) and Customers | CISA

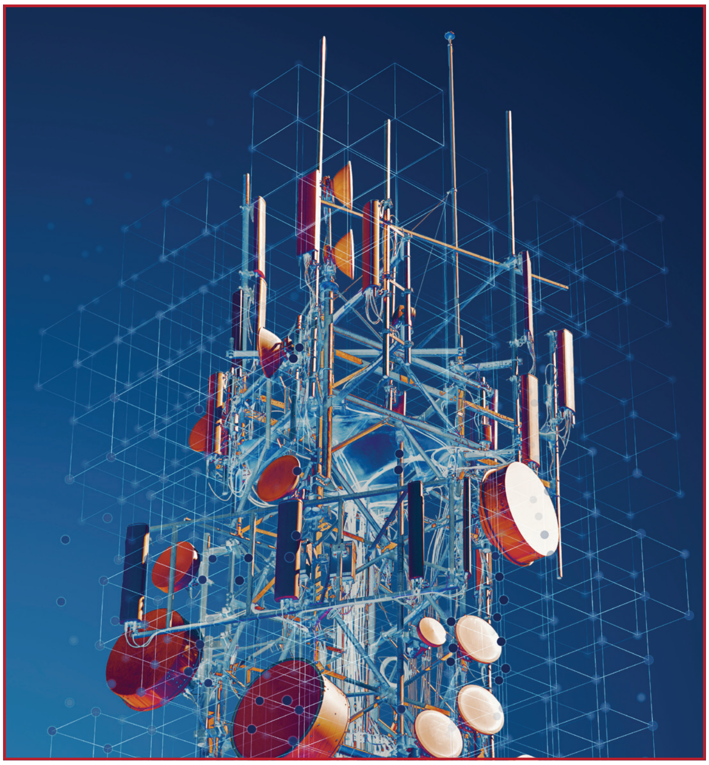
[87] Defending-Telecom-Operators-Against-Nation-State-Threats-FINAL.pdf (hardenstance.com)

[88] https://www.vice.com/en/article/z3xpm8/company-that-routes-billions-of-text-messages-quietly-says-it-was-hacked & https://thestack.technology/vodafone-supplier-hacked-syniverse-hack/

[89] https://www.t-mobile.com/news/network/cyberattack-against-tmobile-and-our-customers

- According to N-able, almost all managed service providers have suffered a successful cyber attack in the past 18 months, and 90% have seen an increase in attacks since the pandemic started[90].
- Successful traffic steering attacks through the border gateway protocol (BGP) compromise[91] of Facebook and content delivery networks[92].
- An operator reported it was the victim of an SMS firewall bypass when fraudsters manipulated SMS signalling while hiding behind a leased global title (GT)[93].

Interconnect attacks, in part, rely on the legacy trust relationships between operators, but this trust can no longer be assumed. The GSMA has published guidance for its members on how to reduce the risk associated with interconnect signalling, particularly in relation to deploying and using SS7 and DIAMETER signalling firewalls. For 5G, the standardisation of a secure edge protection profile (SEPP) has the potential to significantly improve roaming security. The GSMA's Global Title Leasing Task Force is working on recommendations to tackle abuse enabled by GT leasing. The GSMA has also established the Tackling Serious Adversaries Through Interconnect Security Improvement (TSATSI) programme. This cross-mobile industry programme aims to help protect mobile operators and their industry partners from the most serious attacks and threat actors.



[90] State of the Market: The New Threat Landscape | N-able

[91] https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/

[92] From 2020, The incident affected more than 8,800 internet traffic routes from 200+ networks, and lasted for about an hour. Impacted companies are a who's who in the cloud and CDN market, including big names such as Google, Amazon, Facebook, Akamai, Cloudflare, GoDaddy, Digital Ocean, Joyent, LeaseWeb, Hetzner, and Linode. See https://www.zdnet.com/article/russian-telco-hijacks-internet-traffic-for-google-aws-cloudflare-and-others/

[93] GSMA Mobile Industry Intelligence

10 Supply Chain

In light of the serious geopolitical events in 2022, governments and national regulators are trying to increase the resiliency in network infrastructure by placing requirements on all operators to increase the levels of security and controls. This can include new supply chain arrangements to manage operators' use of specific suppliers. A recurring feature is to require the active management of an operator's supply chain. Operators need to consider the 'depth' of management and 'deep understanding' of supply chains required to ensure they are resilient and diverse[94].

Ongoing government interventions, such as the US Entity Listing of Vendors,[95] have both direct (e.g. effectively banning use of certain vendors) and indirect supply chain effects (e.g. limiting use of intellectual property affecting support and electronic component supplies). Vendor selection is also important when considering managed service providers and providers of non-network product (or underpinning) related services, such as cloud providers. It is crucial to understand the business reliance on these aspects, as third parties increasingly deliver some parts of the security and operational models and this introduces new threat vectors. The opportunity for indirect attacks through supplier or third-party tooling and services should not be underestimated and requires vigilance in relation to which third-party tools to use, as well as awareness of the security posture of the third party. The force multiplier effect for an attacker across all the target's customers makes using a compromised vendor an attractive attack proposition.

One of the most concise of recent documents covering this topic is the US CISA, NSA, FBI and international cyber authorities' Cyber Security Advisory to Protect Managed Service Providers and Customers[96] (as previously referenced in the Interconnect Attacks section). The Canadian Centre for Cyber Security has published Cyber Security Considerations for Consumers of Managed Services[97], which contains additional guidance. The UK's National Cyber Security Centre has released a guide: How to assess and gain confidence in your supply chain cyber security - Practical steps to help medium to large organisations gain assurance about the cyber security of their organisation's supply chain.[98]

[94] Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (nist.gov)

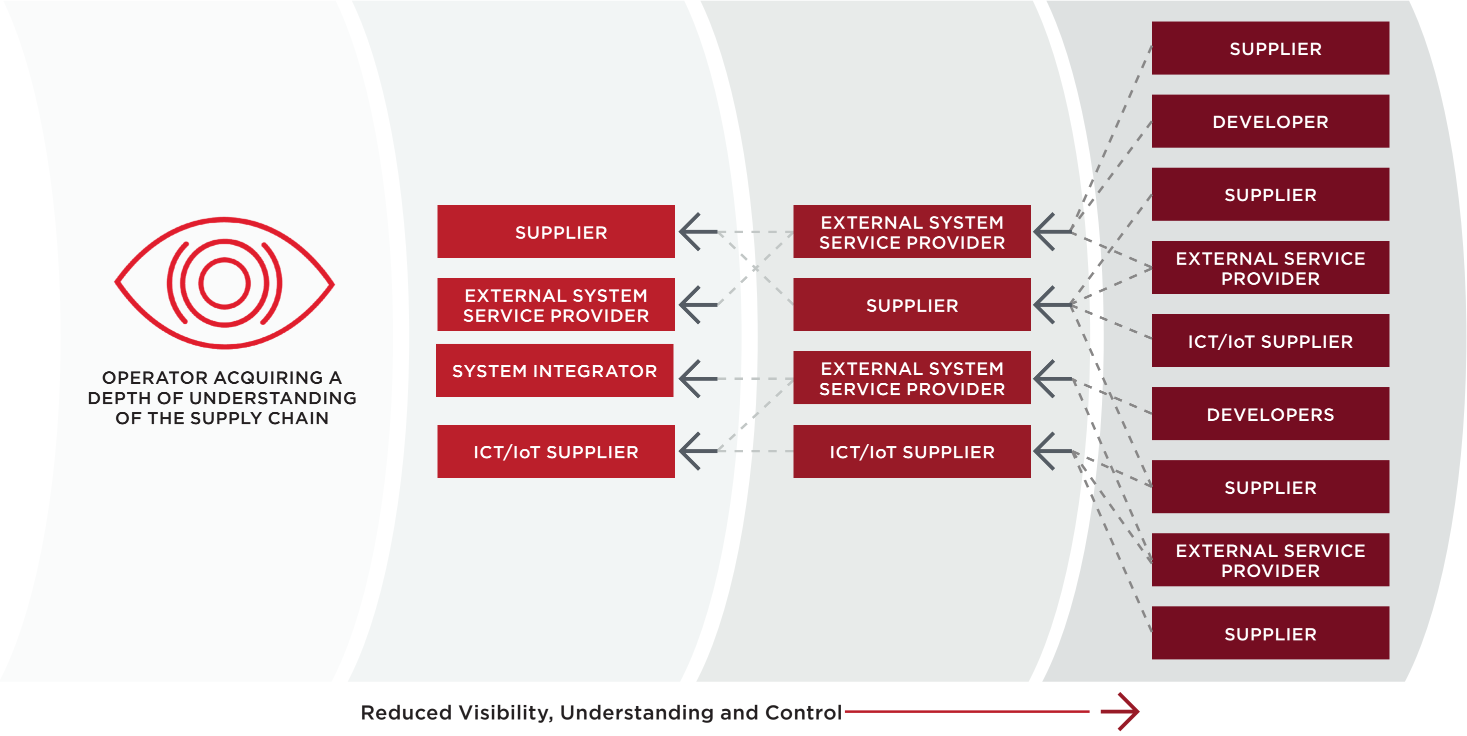
[95] Entity List | U.S. Department of Commerce

[96] CISA, NSA, FBI and International Cyber Authorities Issue Cybersecurity Advisory to Protect Managed Service Providers (MSP) and Customers | CISA

[97] Cyber Security Considerations For Consumers of Managed Services (ITSM.50.030)

[98] https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security

Based on Figure 1.2 from NIST SP 800-161r1


OPERATOR ACQUIRING A DEPTH OF UNDERSTANDING OF THE SUPPLY CHAIN
SUPPLIER
EXTERNAL SYSTEM SERVICE PROVIDER
SYSTEM INTEGRATOR
ICT/IoT SUPPLIER
EXTERNAL SYSTEM SERVICE PROVIDER
SUPPLIER
EXTERNAL SYSTEM SERVICE PROVIDER
ICT/IoT SUPPLIER
SUPPLIER
DEVELOPER
SUPPLIER
EXTERNAL SERVICE PROVIDER
ICT/IoT SUPPLIER
DEVELOPERS
SUPPLIER
EXTERNAL SERVICE PROVIDER
SUPPLIER
Reduced Visibility, Understanding and Control

Supply chain-related security threats reported in 2022:

- According to N-able (as previously referenced), almost all managed service providers have suffered a successful cyberattack in the past 18 months[99].
- Okta reported that during a five-day window of time between January 16-21, 2022, an attacker (Lapsus$) had access to an Okta support engineer's laptop[100].
- Lapsus$ claimed to have leaked NVIDIA's official code signing certificates[101].
- Reported use of rogue Python libraries to steal information, such as credentials, and in June 2022 pygrata and loglib were found to extract AWS keys[102].
- Although the previously reported Log4j library Log4Shell vulnerability[103] was partly addressed during 2022, there remains a range of aligned open source software security threats[104].

The variety of significant supply chain incidents and supply chain threats has prompted a range of government responses and publication of best practices that aim to mitigate supply chain risks. These are notably in the managed service provider area where there may have been inherent customer/supplier and/or partner trust arrangements rather than explicit and enforced security requirements. The US has led efforts to standardise and utilise software bills of materials (SBOMs) as a means to achieve cleaner equipment and software supply chains.

[99] https://www.n-able.com/resources/state-of-the-market-the-new-threat-landscape
[100] https://www.okta.com/blog/2022/03/updated-okta-statement-on-lapsus/
[101] https://analyticsindiamag.com/lapsus-hack-leaves-nvidia-in-a-tight-spot/
[102] https://blog.sonatype.com/python-packages-upload-your-aws-keys-env-vars-secrets-to-web & ENISA Threat Landscape 2022 — ENISA (europa.eu)
[103] https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know
[104] https://portswigger.net/daily-swig/open-source-software

11 Attacks on Virtualised and Cloud-hosted Infrastructure

With the implementation of 5G, the industry is seeing a migration to cloud-based network elements and infrastructure. As a result, security considerations that were once the responsibility of the network equipment vendor may become that of the mobile operator. Since the software is now able to run on a range of non-proprietary platforms, operators need to ensure that whatever combination of hardware and software they use, it stays secure. This includes ensuring that the software is up-to-date, is running on original and authentic hardware and that it has not been altered.

Although cloud-native networks bring a range of opportunities and benefits, including network slicing, network scalability and greater flexibility of vendor choice, they also introduce a range of potential security threats. Containers provide a process-level separation between workloads that can make them quick and cheap to deploy. The underlying kernel and resource scheduling is shared between every container running on the host within the same trust domain. However, a single kernel-level vulnerability might allow an attacker to impact the underlying host and, therefore, all concurrent containers. Potential threats include unauthorised cross-communication between software components, such as containers, memory modification attacks on hardware, undermining the hypervisor and attacks on APIs.

Useful publications on this topic include:

- State of the Cloud: A Security Perspective[105] which provides a perspective driven by operational experience.
- CIS Controls Cloud Companion Guide[106] which provides guidance on how to apply the security best practices found in CIS Controls Version 8 to a variety of cloud environments.
- Cloud Threat Report Vol 3: which describes recent findings across four areas of cloud security: cloud security posture, vulnerabilities and software supply chain, runtime threats and Linux malware and proactive defence and intelligence (including Canary Tokens)[107].
- Red Hat's latest edition of the State of Kubernetes security report[108], which analyses emerging trends in container, Kubernetes, and cloud-native security.

[105] https://www.informationweek.com/whitepaper/cloud-security/cybersecurity/state-of-the-cloud-a-security-perspective/438333
[106] https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
[107] https://info.lacework.com/cloud-threat-report.html?utm_source=website&utm_medium=whitepaper&utm_campaign=website-resources
[108] https://www.redhat.com/en/resources/state-kubernetes-security-report
[109] Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA
[110] Unit 42 Cloud Threat Report, 2H 2021 - Palo Alto Networks

Cloud-related security threats reported in 2022:

- Microsoft's security briefing[109] relating to NOBELIEUM attacks on cloud services (and its previous attack on Solarwinds).
- Unit 42's Cloud Threat Report[110] which asserted that 63% of third-party code used in building cloud infrastructure contained insecure configuration and 96% of third-party container applications deployed in cloud infrastructure contain known vulnerabilities.
- Dark Reading reported a growing threat to VMware ESXi Environments[111], noting two ransomware variants named Luna and Black Basta.
- Karsten Nohl of Security Research Labs announced he had found ways to move from an initial penetration of a cloud instance, to gain sufficient credentials to spy on user communications, extract user data, gain system admin status and ultimately to take down a network[112].

5G is designed to be cloud-native. Cloud and virtualised infrastructure will increasingly be a part of mobile network infrastructure. A successful attack on such infrastructure can have widespread effects at significant scale. There is substantial guidance available to secure virtualised solutions, especially to manage distributed trust relationships. The correct implementation and configuration is key to security.

[109] Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA
[110] Unit 42 Cloud Threat Report, 2H 2021 - Palo Alto Networks
[111] https://www.darkreading.com/attacks-breaches/snowballing-ransomware-variants-highlight-growing-threat-to-vmware-esxi-environments
[112] https://the-mobile-network.com/2022/07/mobile-network-security-researcher-issues-cloud-warning/

12 Human Threat

One of the most important security considerations in any organisation is the human threat (including both inadvertent and deliberate compromises). This can take several different forms associated with the development of a security or fraud attack, some of which also involves social engineering, for example:

- Phishing[113] attacks on a mobile network operator's staff with extensive administration privileges on the operational network in order to compromise their computers, gain credentials, laterally move within the network or gain a foothold for later stages of an attack.
- Tricking, bribing or extorting customer service agents into providing personal customer data or effecting account changes (such as to enable fraudulent SIM swaps).
- A malicious insider who abuses existing accesses and privileges to access data and/or systems, exfiltrate sensitive data, and seek to extend their access/privileges deeper into the network.
- Misconfiguration where a system is left in an insecure default state or misconfigured into an insecure state by mistake, leaving the system vulnerable to attack.
- Highly targeted phishing attacks aimed at senior executives disguised as a legitimate email (so-called 'whaling' attacks).

SoSafe published The Human Risk Review 2022[114], which discusses a human behavioural model and psychological and technical attack vectors that provide further insight into these threats.

Human-related security threats reported in 2022:

- Criminals unsuccessfully attempted to remotely install malware on computers at various operator sales points and partner shops in Europe[115].
- Mobile customers in Europe have received a call without a calling line identifier (CLI) in which the fraudster pretends to be someone else, such as a police officer or government official, and then seeks to extract funds[116].
- A fraudster attempted a SIM swap from an official operator retail shop in Europe by providing counterfeit customer identification, whilst impersonating a real customer and providing a false police report[117].
- Lapsus$ offered a financial bounty to mobile operator experts in return for access to the corporate remote staff virtual private network (VPN)[118].
- A mobile operator in Europe reported several attempts by an unknown actor to contact customer-facing employees via LinkedIn in order to commit fraud[119].

[113] The Anti-Phishing Working Group defines Phishing as "Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials APWG | Unifying The Global Response To Cybercrime

[114] https://lp.sosafe.de/hubfs/SoSafe%20-%20Human%20Risk%20Review%202022%20-%20EN-1.1.pdf

[115] GSMA Mobile Industry Intelligence

[116] GSMA Mobile Industry Intelligence

[117] GSMA Mobile Industry Intelligence

[118] https://securityaffairs.co/wordpress/128912/cyber-crime/lapsus-ransomware-is-hiring.html

[119] GSMA Mobile Industry Intelligence

→ A new technique to bypass two factor authentication was reported called 'prompt bombing'. The attacker triggers authentication requests repeatedly in the hope that the target will authorise a message to make the requests stop[120].

As technical security controls become more effective, the human threat can become the weakest link in the security risk profile. A range of security controls can be established, including staff vetting, additional administrator controls, operating a 'least privilege regime' and education for staff on limiting the content they post on LinkedIn.

Social engineering scams – Case Study

One telco has seen several threat vectors where fraudsters have attempted to socially engineer staff to gain access to and exploit operational systems.

There have been attempts to recruit staff by contacting them via live chat messaging, LinkedIn and personal email. The fraudsters offer to pay staff Bitcoin for information regarding customers with the ultimate goal of having staff complete SIM swaps or email account password resets. Another method to reach the same goal has seen fraudsters asking agents to join Zoom or Microsoft Teams calls, asking the agent to screen share and then giving control of their computer to the fraudster.

Some of the more complex social engineering scams have seen fraudsters call agents and try to trick them into believing they are calling from the telco's own IT department. They direct staff to URLs that are clones of legitimate telco login pages and ask the agents to login with a view to harvesting their login credentials.

[120] https://merchantriskcouncil.org/news-and-press/mrc-blog/2022/what-you-need-to-know-about-prompt-bombing

13 Building Mobile Resilience

The main purpose of a mobile network operator's security architecture should be to preserve three key attributes: confidentiality, integrity and availability. In mobile network architectures, as data is processed, stored or transmitted to and from different components of a network or networks, maintaining 'defence-in-depth' throughout is vital to achieve resilience and security.

Each of the sections within this security landscape report identifies significant threats observed during 2022. The GSMA continues to build security resilience by providing a range of advice, guidelines, recommendations, working activities, discussion fora and threat mitigations; some of which are outlined below. It is through these activities that the GSMA makes an ongoing contribution and provides leadership in mobile network security.

Fraud and Security Working Group

The GSMA's Fraud and Security Group (FASG)[121] drives the GSMA's management of fraud and security matters related to mobile technology, networks and services. The group has two primary objectives. The first is to maintain or increase the protection of mobile operator technology and infrastructure. The second is to maintain or increase the protection of customer identity, security and privacy, such that the mobile industry's reputation stays strong and mobile operators remain trusted partners in the ecosystem. FASG provides an open, receptive and trusted environment within which fraud and security intelligence and incident details can be shared in a timely and responsible way. Members gain from the significant body of knowledge published on fraud and security matters. FASG has a number of sub-groups including the Fraud and Security Architecture Group, the Device Security Group, the Roaming and Interconnect Fraud and Security Group and the Security Assurance Group.

During 2022, FASG provided recommendations and guidance to network operators and key industry suppliers on roaming and interconnect security issues to ensure its advice remains current and effective. These include best practice advice on the use of signalling firewalls and a fraud and security assessment of flash calling. The Device Security Group updated the GSMA requirements for installing security critical software patches (FS.25) on mobile devices to enhance protection for users, updated the GSMA's security algorithm deployment guidance and enhanced mobile device blocking and data sharing recommended practice.

Tackling Serious Adversaries Through Interconnect Security Improvement (TSATSI) programme

TSATSI is a cross-industry programme to help operators and industry partners protect themselves from the most serious attacks and threat actors. The aim is to create a hostile environment for attackers and a mesh of security across the mobile industry, providing strength-in-depth throughout.

[121] https://www.gsma.com/aboutus/workinggroups/fraud-security-group

Telecommunication Information Sharing and Analysis Center (T-ISAC)[122]

The GSMA T-ISAC is the central hub of security information sharing for the telecommunication industry. Driven by the ethos "one organisation's detection is another's prevention", the T-ISAC operates on the principle that information sharing is essential for the protection of the mobile ecosystem, and the advancement of cyber security for the telecommunications sector. Drawing on the collective knowledge of mobile operators, vendors and security professionals, the T-ISAC collects and disseminates information and advice on security incidents within the mobile community – in a trusted and anonymised way.

Coordinated Vulnerability Disclosure Programme (CVD)[123]

The GSMA CVD programme gives security researchers a discreet route to disclose a vulnerability, affording the industry an opportunity to assess the impact and mitigation options, before details of the discovered vulnerabilities enter the public domain. The programme works with mobile operators, suppliers and standards bodies to develop fixes and mitigating actions to protect customers' security and trust in the mobile communications industry.

Security Accreditation Scheme[124]

The Universal Integrated Circuit Card (UICC) in mobile devices, and its associated applications and data play a fundamental role in ensuring the security of the subscriber's account and related services and transactions. The GSMA's Security Accreditation Scheme enables mobile operators to assess the security of their UICC and embedded UICC (eUICC) suppliers, and of their eUICC subscription management service providers.

During 2022, the scheme was updated to permit certification of secure cloud-service provider-managed Hardware Security Modules by subscription management service providers and scheduled releases were introduced to enable controlled development of the Security Accreditation Scheme requirements.

Network Equipment Security Assurance Scheme[125]

The Network Equipment Security Assurance Scheme (NESAS), jointly defined by 3GPP and the GSMA, provides an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry. NESAS defines security requirements and an assessment framework for secure product development and product lifecycle processes, as well as using 3GPP-defined security test cases for the security evaluation of network equipment. NESAS provides a security baseline to evidence that network equipment satisfies a list of security requirements and that the equipment has been developed in accordance with vendor development and product lifecycle processes that provide security assurance. NESAS is intended to be used alongside other mechanisms to ensure a network is secure. The scheme has been designed to be used globally as a common baseline, on top of which individual operators or national IT security agencies may want to define additional security requirements.

Two new releases of NESAS were published in January 2022 and October 2022 that enhanced the scheme based on feedback and operational learnings. Additional guidance for vendors and auditors on the conduct of NESAS audits and for vendors and test labs on the performance of NESAS product evaluations were also published and a NESAS Oversight Board was established to enhance scheme governance.

[122] https://www.gsma.com/security/t-isac/
[123] https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/
[124] https://www.gsma.com/security/security-accreditation-scheme/
[125] https://www.gsma.com/security/network-equipment-security-assurance-scheme/

eUICC Security Assurance[126]

The GSMA eUICC Security Assurance (eSA) scheme is an independent security evaluation scheme for evaluating embedded UICCs (eUICCs) against the provisions of protection profiles for eUICCs. The scheme aims to establish trust for service providers and other risk-owners that their assets, including profiles for eUICC remote provisioning, are secure against state-of-the-art attacks. The scheme is based on the 'common criteria' methodology, optimised for GSMA-compliant eUICCs.

Post-Quantum Telco Network Taskforce[127]

The GSMA Post-Quantum Telco Network Taskforce will help define requirements, identify dependencies and create the roadmap to implement quantum-safe networking, mitigating the potential risks arising from the powerful quantum computers of the future. Without quantum-safe controls in place, sensitive information such as confidential business information and consumer data, could be at risk from attackers who harvest present-day data for later decryption.

Securing the 5G Era[128]

5G was designed with security controls to address many of the threats faced in legacy 4G/3G/2G networks. These controls include new mutual authentication capabilities, enhanced subscriber identity protection and additional security mechanisms. 5G offers the mobile industry an unprecedented opportunity to uplift network and service security levels. 5G provides preventative measures to limit the impact of known threats, but the adoption of new network technologies also introduces potential new threats for the industry to manage. The GSMA is exploring a range of security considerations including secure-by-design, 5G deployment models and 5G security activities.

The GSMA's 5G Security Taskforce exists to manage and track 5G security-impacting work items within the GSMA, and externally. In the course of 2022 members contributed to a number of important 5G security initiatives related to 5G roaming, addressing structures for SEPPs (security edge protection proxies), defining certificate hierarchies and developing tools to enable key and certificate hosting.

GSMA Security Publications[129]

The GSMA security website includes a number of informative and instructive publications, whilst GSMA members can exclusively access additional content specifically addressing a wide range of fraud and security topics. In addition to the FASG publications mentioned above, advice on voice mail security and binary SMS filtering were updated in 2022, guidelines were published on the use of the GBA mechanism to practically implement online certificate provisioning for a range of IoT and M2M scenarios. The GSMA also published guidance for members on risks related to artificial intelligence (AI) technology, further adding to the valuable cannon of the GSMA security output.

[126] GSMA | GSMA eUICC Security Assurance: Test. Trust. Assure. - Services
[127] GSMA | GSMA, IBM and Vodafone Establish Post-Quantum Telco Network Taskforce - Newsroom
[128] https://www.gsma.com/security/securing-the-5g-era/
[129] https://www.gsma.com/security/

Final Thoughts

This document provides an overview of the security landscape for the mobile industry in the context of current threats facing mobile network operators, their customers and the wider ecosystem. This year's report has outlined a range of threat types from the human threat, through to ransomware, destructive wiperware and how mobile networks can play a supporting role during times of conflict. Although some of these threats are new, many of them are pre-existing or re-packaged threat variants. Mitigation recommendations and effective responses exist and are available for implementation. Rapid intelligence sharing by industry participants to counter these threats in an efficient manner is crucial.

The topics covered in this report are summarised in the graphic below:

Themes

- Infiltration
- Exploiting Access
- Compromising Service Ability

Attack Types

- Ransomware
- Malware
- Smishing
- Spyware
- Critical National Infrastructure Attacks
- SIM Swap
- eSIM Fraud
- Interconnect Attacks
- Supply Chain
- Attacks on Virtualised and Cloud-hosted Infrastructure
- Human threat

Building Security Resilliance

- GSMA Security Working Groups
- GSMA Best Practices
- T-ISAC
- CVD
- SAS
- NESAS
- Securing 5G
- TSATSI
- GSMA Publications

This report also highlights the GSMA's role in supporting the mobile industry to build greater security resilience. The GSMA recommends industry stakeholders make active contributions to build and augment GSMA security guidance and recommendations, while implementing existing industry requirements and best practices.

Over the coming year, the GSMA will continue to support its members on security matters.
To get in touch, or to get more closely involved, please email security@gsma.com.