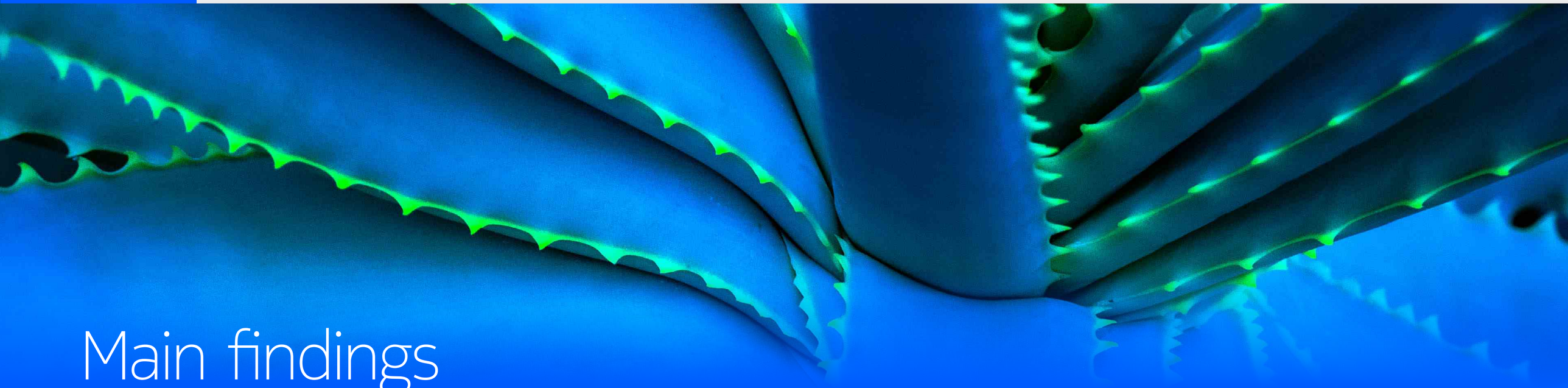
NOKIA

Threat Intelligence Report 2023

Identifying attack trends to protect telecom networks and customers' data



Main findings

Attacks on mobile networks

- 60% of attacks in telecom mobile networks are linked to Internet of Things (IoT) **bots scanning for vulnerable hosts** to expand their botnets for use in distributed denial-of-service (DDoS) attacks.
- Communications service providers (CSPs) are struggling to keep up with the latest threats. More than 30% of CSP respondents to a Nokia/GlobalData survey said they had experienced **eight or more breaches in the last 12 months**.
- More than half of the CSP respondents said **fragmented tools** make it difficult to effectively implement security capabilities across various systems and use cases.
- CSPs are carefully considering **geopolitical developments** when evaluating and mitigating security risks.

Malware attacks

- In total, more than one-third (35%) of the malware attacks detected were either **ad-click bots, crypto-miners or banking trojans** (15%, 11% and 9%, respectively).
- While adware decreased by 25%, crypto-mining kept stable and **banking trojans almost doubled**, climbing from 5% in 2021 to 9% in 2023.
- **Residential malware infection rates** continue to decline, falling from 3% to 1.5% — but still remain above the pre-pandemic rates of 1%.

DDoS attacks

- The rise of **IoT and cloud technologies** in both residential and enterprise networks has contributed significantly to the expansion of botnets.
- **Botnets have become a major generator of DDoS traffic**. Between 500,000 and 1,000,000 globally distributed, remotely controlled IoT hosts or cloud server instances are active daily, generating more than 40% of all DDoS traffic.
- **DDoS attacks are becoming "weaponized"** as larger and more powerful botnets are used by state actors and co-opted into geopolitical conflicts.
- In 2023, 90% of **complex, multi-vector DDoS attacks** were based on botnets.

Mobile network attack trends

In a 5G world, cybersecurity is needed more than ever to protect networks, data and users from threats. Cyber threat intelligence (CTI) plays an important role in providing an in-depth understanding of potential threats to mobile networks, including malicious actors and their motivations — valuable information that can be used to strengthen the security measures of CSPs.

At the Cybersecurity Center in France, we rely on several data sources to inform our CTI capabilities and develop effective countermeasures:

- We leverage numerous threat intelligence feeds from trusted industry sources, which provide real-time information about emerging threats and vulnerabilities to telecom networks.
- The expert team in our Cyber Threat Intelligence Center plays a pivotal role in curating and analyzing relevant data, sifting through vast amounts of information to identify trends and provide actionable intelligence to CSPs.
- We are a member of the GSMA Telecommunication Information Sharing and Analysis Center (T-ISAC), a collaborative platform that allows us to tap into the collective knowledge of industry experts and gain new insights into emerging threats specific to the telecom industry community.

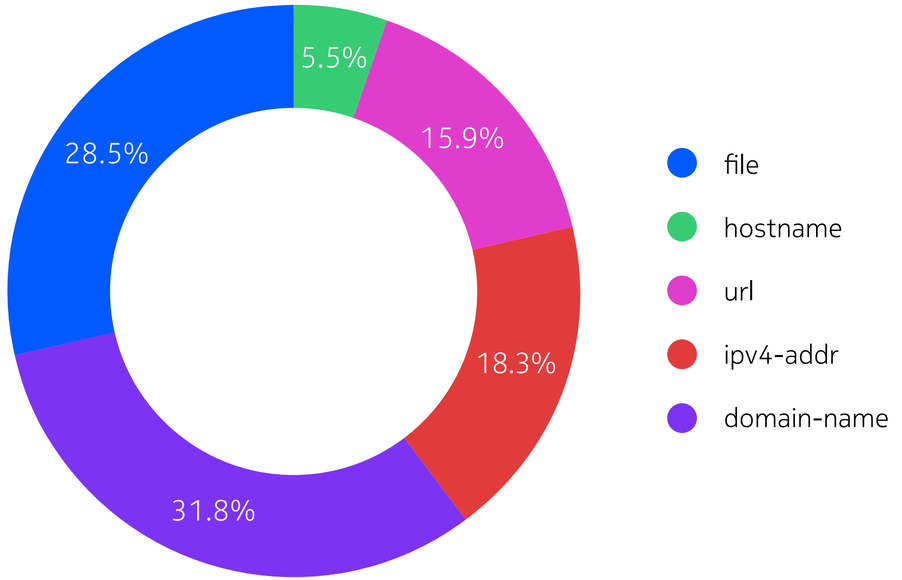
Together, these diverse sources of information form a robust framework for gathering and analyzing CTI — and for empowering CSPs with the knowledge necessary to proactively defend against evolving threats in the 5G era.

Attack trends

Top attack vectors

The telecom industry faces threats from many potential attack vectors, with the top five currently being domain name, file, IP, URL and hostname, as shown in Figure 1. The high percentage of file and IP indicators reflects the continued use of malware- and network-based attacks, while URL and hostname indicators suggest web-based attacks and domain name system (DNS) hijacking continue to be threats.

Figure 1. Top attack vectors



Top threat actors

There are several threat actors that have been actively targeting the telecom sector for more than 10 years and continue to be observed by our team. As shown in Table 1, the number of threat actors has grown considerably since 2012.

These threat actors use a broad range of tactics, techniques, and procedures — including phishing, social engineering, and exploiting vulnerabilities in software and hardware — to breach the networks of CSPs and gain access to sensitive data such as call records, subscriber information and network configuration details. Attacks often involve the use of sophisticated malware and backdoors to gain persistent access to target networks, allowing the threat actors to carry out their operations undetected for extended periods.

Table 1. List of threat actors targeting telecom sector

First seen	Name	Targets
2012	Gallium	Telecom companies, financial institutions and governments in Asia
2013	Tonto Team	Telecom companies, governments and other victims in Asia and Eastern Europe
2013	Gamaredon	Militaries, law enforcement agencies and telecom companies
2015	APT 42	Individuals and organizations of strategic interest to Iran
2016	Calypso	Telecom company in Afghanistan
2016	LightBasin	Telecom companies
2017	Hexane	Internet service providers and telecom companies in Africa, the Middle East and Asia
2017	BackdoorDiplomacy	Telecom companies in the Middle East
2019	DecisiveArchitect	Telecom companies and other global entities
2022	Metador	Telecom companies, internet service providers and universities in the Middle East and Africa
2022	Roaming Mantis	Governments and telecom companies in Africa, Europe, the Middle East and Asia
2022	WIP19	Telecom companies and IT service providers in the Middle East and Asia
2022	Scattered Spider	Telecom and business process outsourcing (BPO) companies
2023	Operation Tainted Love	Telecom companies

Learnings and recommendations

By staying informed of the latest attack trends, CSPs will be better able to implement effective security strategies to protect their networks and their customers' data.

5G network attacks

As technology advances, so do the methods and tactics of cyber attackers. In the year ahead, some of the predicted threats to telecom networks resulting from the adoption of 5G include:

- **Exploitation of 5G network slicing:** Attackers may attempt to compromise one slice and then move laterally to other slices or the core network, potentially gaining access to sensitive information or disrupting critical services.
- **Use of 5G networks as a platform for large-scale DDoS attacks:** Attackers may be able to launch more powerful attacks than ever before due to the increased bandwidth and low latency of 5G. Additionally, the proliferation of IoT devices is creating a larger attack surface that can be exploited.
- **5G supply chain threats:** The adoption of 5G has led to the unprecedented convergence of the IT and telecom worlds — and a multitude of new technologies operating in the core of the telecom networks. This increases the potential for malicious actors to target the growing supply chain of vendors and subcontractors who now have access to sensitive information or critical systems, exploiting these third-party relationships to gain entry into telecom networks.

To defend against these threats to their 5G networks, CSPs must have a comprehensive and proactive security strategy in place that includes:

- **Advanced threat detection and response:** Given the dynamic and complex nature of 5G networks, real-time visibility into traffic and the ability to detect and respond to threats as quickly as possible is critical.
- **Cyber threat intelligence:** As CSPs implement a robust cybersecurity cycle, CTI will play a vital role in collecting and analyzing relevant information about potential threats, vulnerabilities and attacker tactics.
- **Strong access controls and user management:** To mitigate the risks posed by supply chain threats, CSPs should conduct thorough due diligence on their suppliers and vendors, and implement strict security controls for all third-party network access. This includes:
  - **Multi-factor authentication:** Requiring users to provide two or more verification factors can help prevent unauthorized access to sensitive systems or data.
  - **Role-based access control:** Limiting user access to only the resources they need to perform their jobs can help minimize the extent to which a threat actor can penetrate the network.
  - **Privileged user monitoring:** Regularly reviewing privileged user activity can help detect and prevent unauthorized actions or data exfiltration.
- **Regular vulnerability assessments and penetration testing:** Performing these kinds of tests on a regular basis can help identify and address potential security weaknesses in 5G networks before they can be exploited by attackers.

IT/supply chain attacks

In addition to 5G, several other key attack trends are predicted to continue to pose an ongoing threat to the telecom industry in 2023, including:

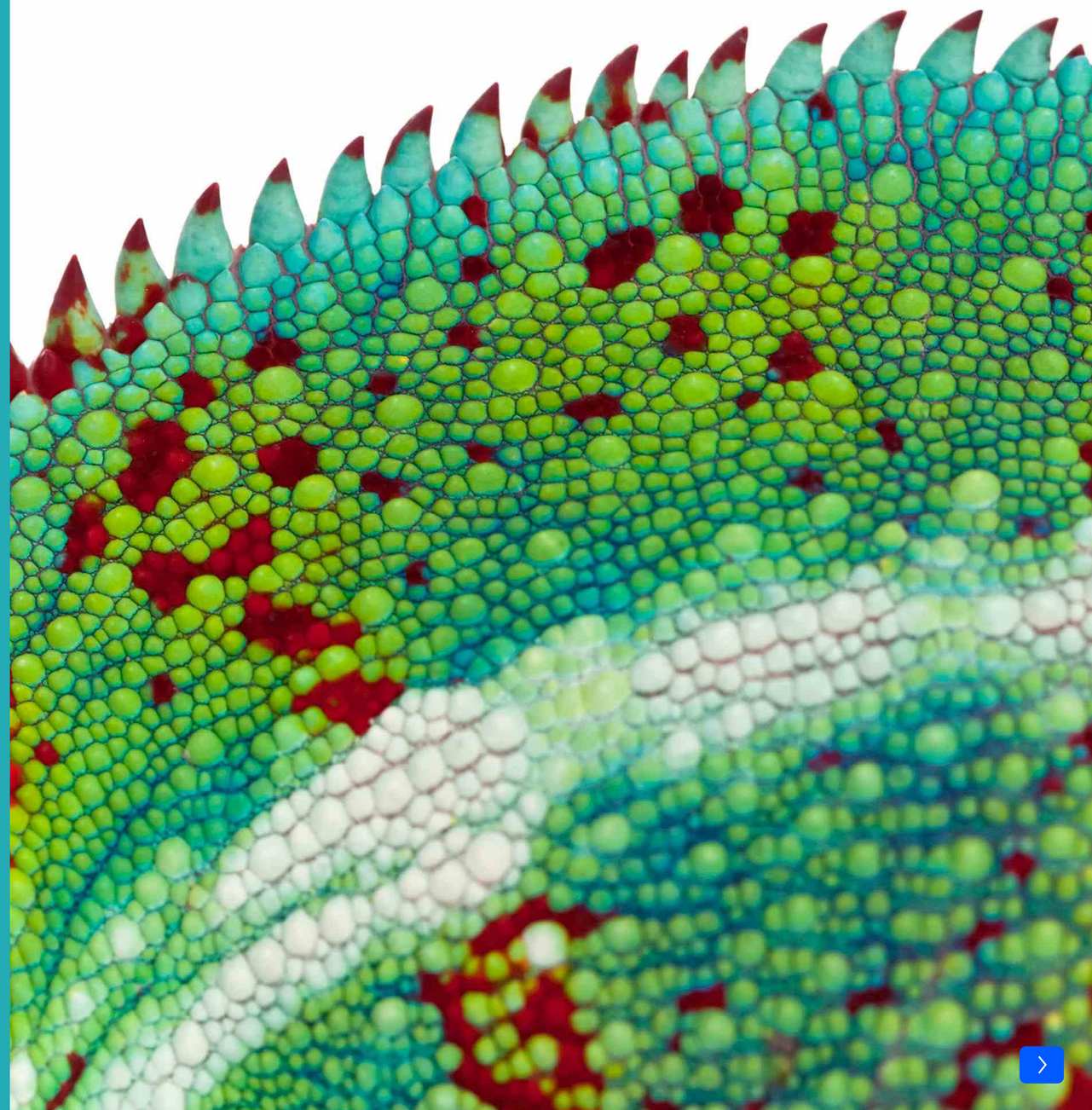
- **Ransomware:** Threat actors are using more sophisticated and targeted ransomware attacks against the telecom industry, leveraging zero-day vulnerabilities and exploiting weak passwords to gain access to networks. CSPs should implement multi-factor authentication and regularly back up their data to mitigate the impacts of a successful ransomware attack.
- **IoT devices:** The proliferation of IoT devices has created new attack vectors for threat actors. IoT devices are often not as secure as traditional IT assets, making them vulnerable to botnets and DDoS attacks. CSPs should implement device-level security controls and monitor their network traffic for unusual activity.
- **Insider threats:** Employees with access to sensitive data can cause significant damage if their credentials are compromised or if they engage in intentionally malicious activity. CSPs should implement strict access controls and employee training programs to mitigate the risk of insider threats.

5G threat intelligence framework

A threat intelligence framework provides a comprehensive approach for characterizing and categorizing threats by focusing on the attack phases, tactical objectives and techniques used by threat actors. Up to now, most frameworks were developed with traditional IT systems in mind. That changed in September 2022, when MITRE and the US Department of Defense launched the FiGHT (5G Hierarchy of Threats) framework, making it possible to reliably assess the confidentiality, integrity and availability of 5G networks as well as the devices and applications using them.

The launch of the FiGHT framework is a significant milestone for the telecom industry, as it allows stakeholders to assess where cybersecurity investments will have the highest impact as they build, configure and deploy 5G systems. The FiGHT framework will be particularly valuable to CSPs, telecom equipment manufacturers and cybersecurity researchers looking to identify and mitigate potential threats to 5G networks.

Nokia is proud to have been part of the MITRE workgroup that helped develop this important threat intelligence framework for the 5G ecosystem.



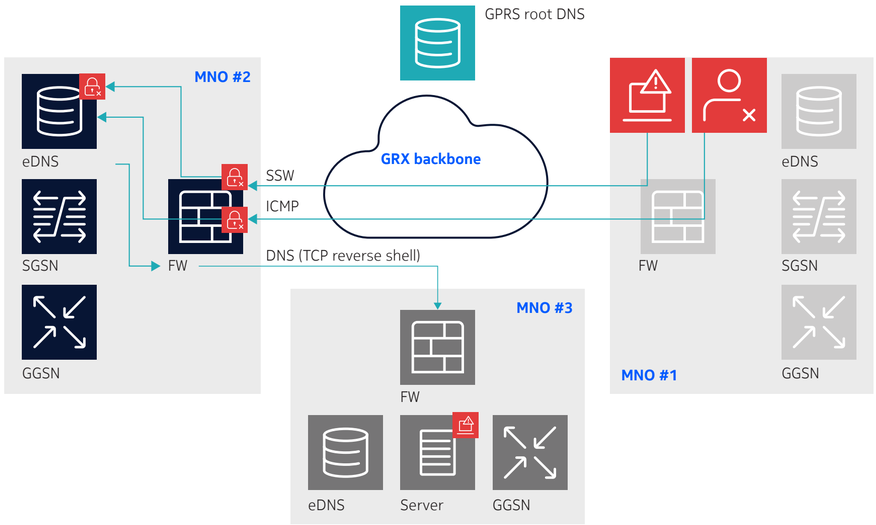
Spotlight: How the FiGHT framework can be used to analyze and prevent attacks

Between 2016 and 2022, the LightBasin group launched several attacks against the telecom sector in Southeast Asia. Using the FiGHT framework, we were able to analyze and identify the tactics, techniques and procedures used by LightBasin, revealing a multi-stage operation involving both bypass vulnerabilities and technical exploits to gain access to CSPs' internal networks and steal customer data.

Specifically, we found two main attack variations:

- **First variation:** The attackers brute-force their way via SSH into an external DNS server (eDNS) of the General Packet Radio Service (GPRS) roaming exchange (GRX) network, then deploy a SLAPSTICK PAM backdoor to steal credentials and move laterally into other systems. From there they target other eDNS servers and use a PingPong implant to establish a TCP reverse shell triggered by a magic Internet Control Message Protocol (ICMP) packet. The TCP reverse shell is linked to an IP address and port specified within the magic ICMP packet, such as port 53, to disguise the activity as ordinary DNS traffic. This allows the attackers to exploit vulnerabilities in the eDNS protocol and launch attacks on GPRS and other mobile networks using techniques such as GPRS Tunneling Protocol (GTP).

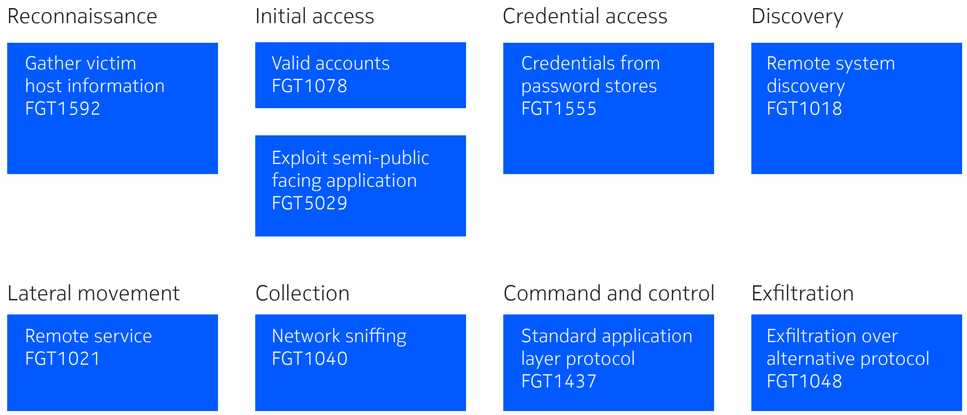
Figure 2. LightBasin attack variation using a TCP reverse shell



- **Second variation:** After brute-forcing their way into an eDNS, the attackers combine the open-source Unix backdoor TinyShell with publicly available software that emulates the Serving GPRS Support Nodes (SGSNs), which allows them to tunnel outbound traffic through the network. A command-and-control script runs on the compromised system and executes specific steps (such as downloading malicious software) during a 30-minute window each day to minimize risk of detection.

The analysis of this attack can be mapped to the FiGHT framework, as shown in Figure 3:

Figure 3. FiGHT matrix of LightBasin tactics and techniques



This mapping process allowed our security analysts to quickly identify the tactics, techniques and procedures used by the attackers, leading to prompt response and risk mitigation.

Overall, the visual nature of frameworks like FiGHT enhances situational awareness, empowers informed decision-making by security teams, and strengthens organizations' resilience against cyber threats. It also enables efficient detection of complex attack patterns, supporting proactive defense strategies and improving incident response capabilities. For instance, we implemented the results of our LightBasin analysis into our own CTI platform, resulting in the following security recommendations for CSPs:

Table 2. Security recommendations from Nokia's analysis of LightBasin attacks

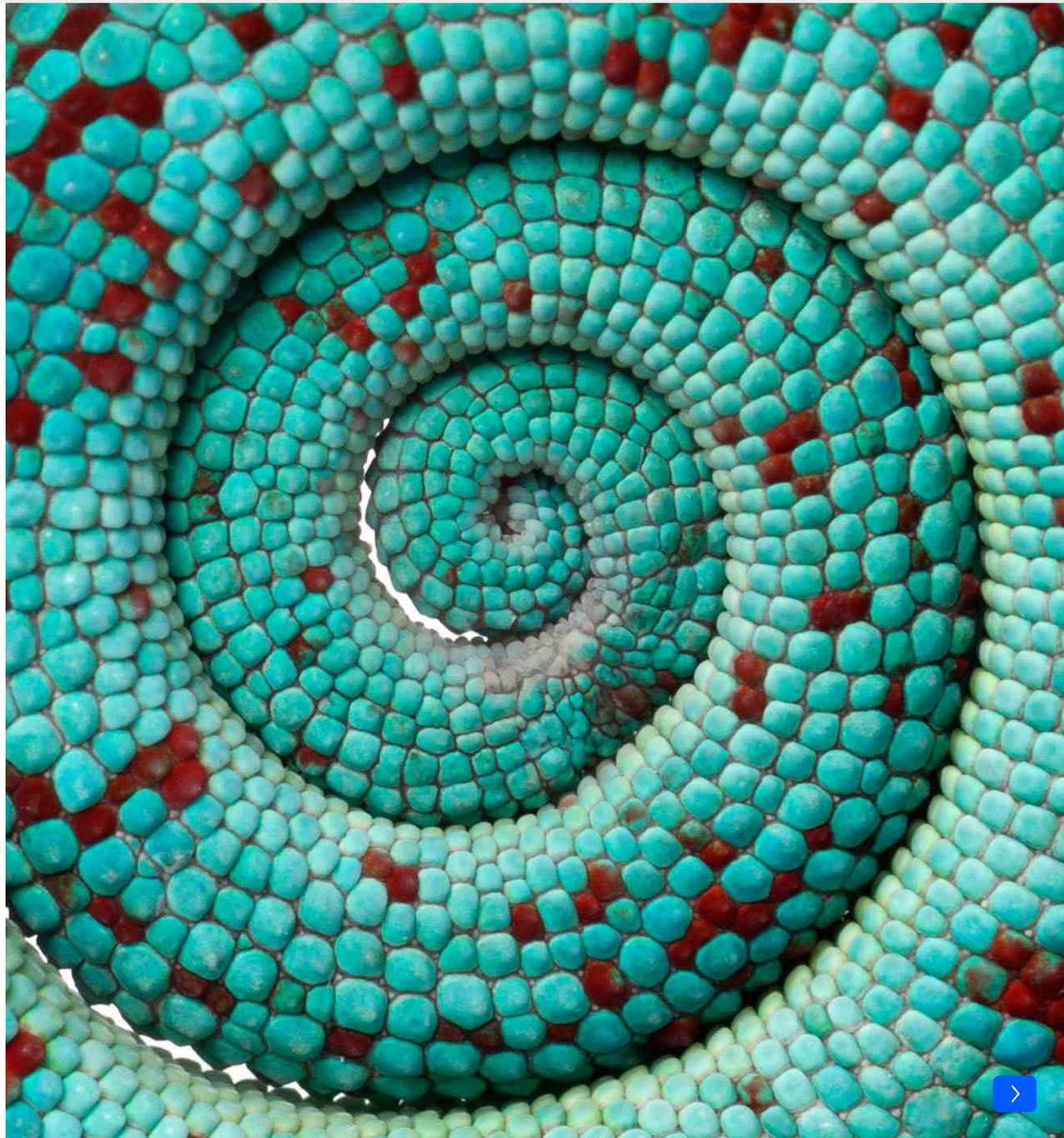
Domain	Recommendation
Asset inventory	Make an inventory of equipment accessible from the GRX network to identify any unauthorized interfaces or network segments.
Provider control	Conduct an evaluation of the security controls in place with third-party managed service providers to ensure their systems are sufficiently protected (as they may manage parts of the network).
EDR and file integrity monitoring	Implement basic security controls and logging on Unix-based operating systems that support core telecom network services, including SSH logging, endpoint detection and response (EDR), and file integrity monitoring (FIM).
Restricted firewall	Put in place firewall rules to restrict network traffic to only expected protocols such as DNS or GTP.
GTP hardening and network-based intrusion detection	Use a number of protocol-specific hardening techniques. Implement GTP tunnel endpoint (GTP TEID) validation, message sequence number validation and replay protection to prevent GTP-based attacks such as tunnel hijacking or session hijacking. Implement DNS security extensions to provide cryptographic authentication of DNS responses and reduce the risk of DNS cache poisoning attacks. Consider GRX as a border, rather than a friendly interface between MNOs, and proceed with securing SS7 and Diameter. Implement GTP IDS to have full visibility of the network and prevent attacks through the GRX layer.
Cyber threat intelligence	Have up-to-date and comprehensive threat intelligence resources to understand the threats facing the industry, including the tactics, techniques and processes used by attackers, then use these insights to augment detection mechanisms and inform security control decisions.

The LightBasin case demonstrates the importance of threat intelligence for the telecom industry. By using frameworks like FiGHT to analyze and understand the methods used by threat actors, CSPs can take proactive measures to protect their networks and safeguard their customers' data.

Malware activity trends

This section of the report provides a view of malware activity in fixed broadband and mobile networks around the world in 2022 and the first quarter of 2023. The data has been aggregated from CSP networks where Nokia NetGuard Endpoint Security solution is deployed. This network-based malware detection solution enables Nokia customers to monitor their networks for evidence of malware infections in consumer and enterprise endpoint devices, including mobile phones, laptops, personal computers, tablets and IoT devices. It is deployed in major fixed and mobile networks around the world, monitoring network traffic from more than 200 million devices.

Nokia NetGuard Endpoint Security also monitors network traffic for malware command-and-control communication, exploit attempts, hacking activity and scanning activity. This enables the solution to accurately determine which devices are infected with malware and what malware is involved. The solution also monitors attack traffic to determine where attacks are coming from and what network devices are being attacked.



Malware in fixed broadband networks

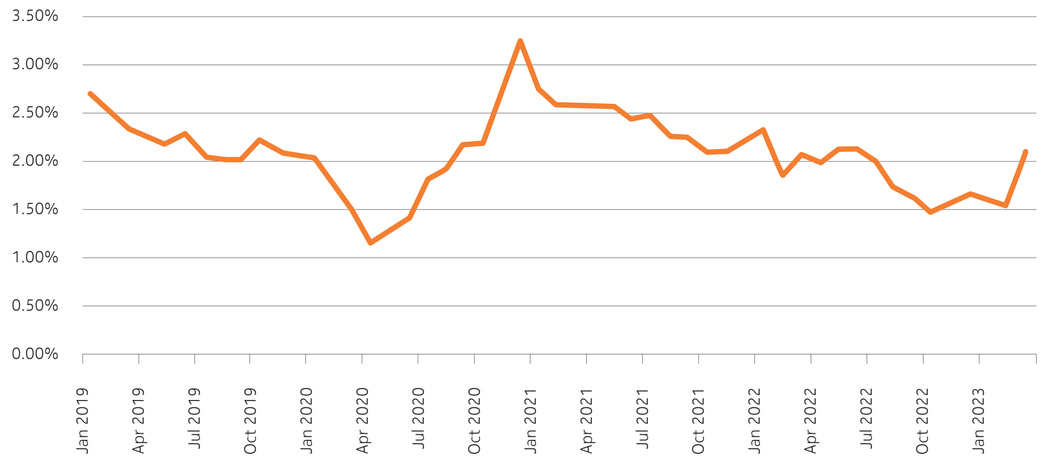
In fixed broadband networks, probes are deployed at peering points to monitor traffic between the internet and residential home networks. This includes any household devices (such as desktop computers, laptops and mobile phones) connected to the household Wi-Fi, as well as any IoT devices talking to the internet.

Overall infection rate

In fixed networks, an "infection" is recorded when traffic from specific malware is identified as coming from a household. This is typically done by detecting command-and-control traffic associated with the malware.

As shown in Figure 4, since 2019, about 2% of households have experienced some sort of malware issue each month. The increase from April 2020 until the end of 2020 coincides with the onset of COVID-19, when many people were working from home. In 2021 and 2022, this trend was reversed and malware infections have since returned to pre-pandemic levels.

Figure 4. Monthly fixed network malware infection rates, January 2019 – January 2023



Top malware

Table 3 shows the top 10 malware identified in fixed broadband networks since the start of 2022.

The most common malware is Adylkuzz.B, a crypto-miner targeting Windows and Linux platforms. The Windows version uses the Eternal Blue vulnerability to spread from host to host. This is followed by Mandrake, an Android banking trojan. It is disguised as a legitimate app that, once installed, steals personal information including access credentials for online banking.

Next is Pareto, an ad-click bot that is integrated into seemingly legitimate Android apps and games. It generates revenue for its authors by having users click on advertisements. Although this activity does not damage the host, it does consume network resources and battery power.

Rounding out the top four is Adload, which is adware that affects macOS computers and laptops. Masquerading as some kind of utility, once executed, it installs itself into web browser extensions and injects unwanted advertising into web pages.

Table 3. Top 10 malware detected in fixed networks, 2022 and Q1 2023

Rank	Malware name	%
1	Indep.Miner.Adylkuzz.B	11.07
2	Android.BankingTrojan.Mandrake	9.13
3	Android.Bot.Pareto	8.73
4	OSX.Adware.AdLoad	7.08
5	Indep.Bot.Mirai.variants	5.47
6	Win32.HackerTool.TektonIt	3.64
7	Indep.SpamBot.GenericSpam	3.38
8	Win32.Backdoor.NanoCore	3.02
9	Indep.InfoStealer.Formbook	2.41
10	Android.MobileSpyware.mSpy	1.92

Top attacks

Table 4 shows the top 10 attacks on residential networks since the start of 2022.

The vast majority (88%) of attack traffic involves scanning for potentially vulnerable devices. One approach commonly used by IoT bots looking to add more victims to the botnet is scanning for systems that accept SSH connections. Once found, the bot will attempt a brute-force login to compromise the system. Another approach is a generic TCP port scan, which looks for any open TCP port as a precursor to a more specific attack. This is also used by a number of IoT bots as part of their propagation strategy.

The third-most common attack is specifically designed to compromise a Huawei home router. Most residential networks use private IP addresses and are protected from the outside by the home router. As the router is usually the only device visible from the internet, it is a frequent target of attacks.

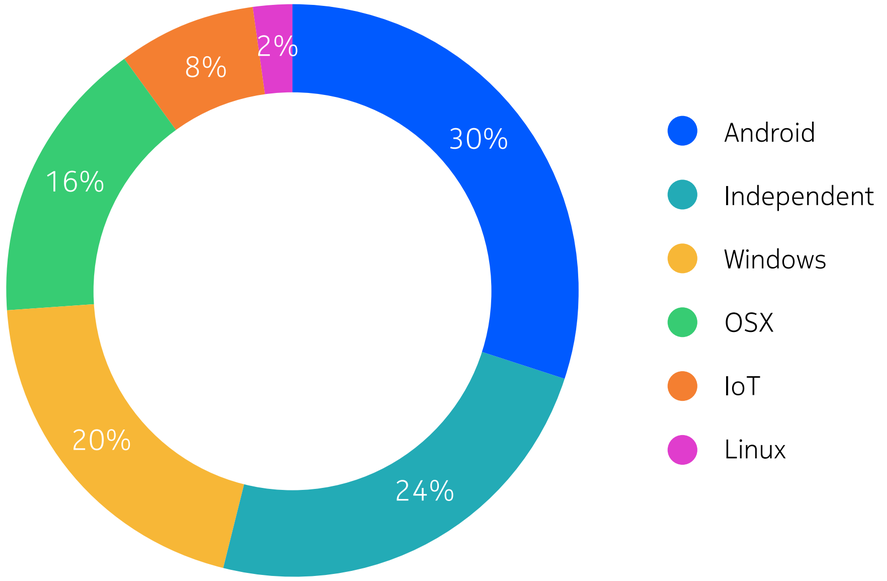
Table 4. Top 10 attacks in fixed networks, 2022-2023

Rank	Malware name	%
1	Excessive SSH connection attempts	47.6478
2	TCP port scanning	41.3641
3	Huawei home gateway exploit (CVE-2017-17215)	10.1767
4	DNS amplification attack	0.6794
5	Realtek Miniigd UPnP SOAP RCE attempts (CVE-2014-8361)	0.0706
6	IoT.Bot.BCMUPnPHunter port scan	0.0231
7	Flood of bad TELNET logins	0.0174
8	NMAP styled network scan	0.0064
9	Potential DNS tunneling (high TXT requests)	0.0058
10	Potential DNS tunneling (high CNAME requests)	0.0032

Infections by device

Figure 5 provides a breakdown of fixed broadband network infections by device type. Phone and home devices using Android OS are responsible for 30% of malware activity. Malware that is platform independent (i.e., it can affect Windows, Linux and a variety of smartphones) accounts for 24% of total infections. This is followed by Windows (20%), OSX (16%), IoT (8%) and Linux (2%) infections.

Figure 5. Fixed network malware infections by device, 2022-2023



Malware on mobile networks

In mobile networks, probes are deployed to monitor user plane traffic in the mobile core network. By using International Mobile Equipment Identity (IMEI) and International Mobile Subscriber Identity (IMSI), we can then uniquely identify specific mobile phones, laptops with mobile dongles, mobile IoT devices, and mobile Wi-Fi routers and hotspots.

Overall infection rate

In mobile networks, an "infection" is recorded when traffic from specific malware is identified as coming from a mobile device. This is typically done by detecting command-and-control traffic associated with the malware.

As shown in Figure 6, the mobile infection rate has stayed at about 0.1% since mid-2020. As most mobile malware can be attributed to trojanized applications, this improvement (when compared to pre-pandemic rates) is likely due to changes in app store security practices that ensure apps are screened for malware before they can be downloaded by users.

Top malware

Table 5 shows the top 10 malware identified in mobile networks since the start of 2022.

The most common mobile malware is a bot that scans the network for devices that accept SSH connections, a tactic associated with a variety of IoT botnets. The fifth-ranked Mirai bot is very similar, meaning two of the top 10 malware are associated with IoT bots scanning for vulnerable hosts to expand the botnet. A number of Android-specific infections also make the top 10, including the Pareto ad-click bot, the Mandrake banking trojan, the Multiverse info-stealer and three Android spyware apps.

Of note is the ZeroAccess botnet, a Windows based peer-to-peer botnet first seen in 2012 but is still infecting mobile devices today.

Figure 6. Monthly mobile network malware infection rates, January 2019 – January 2023

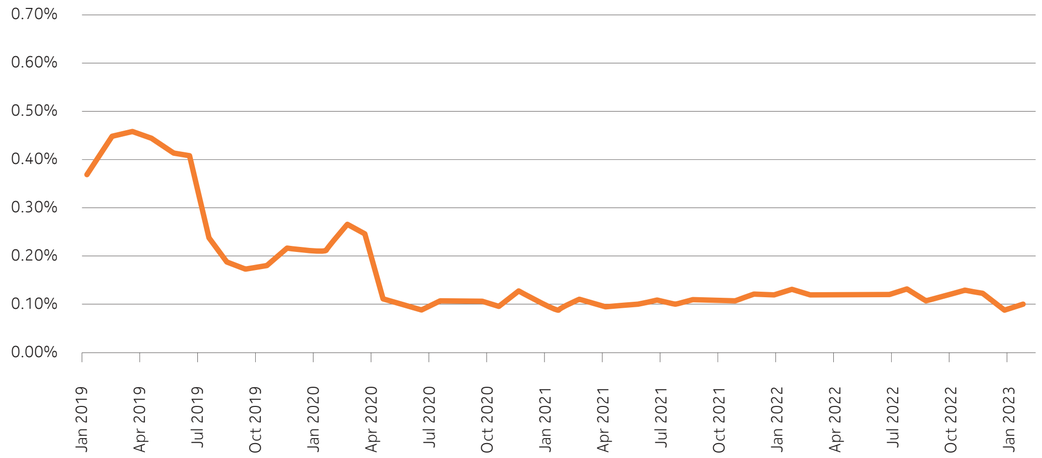


Table 5. Top 10 malware detected in mobile networks, 2022-2023

Rank	Malware name	%
1	Indep.Bot.SshScanBot	19.88
2	Android.Bot.Pareto	13.26
3	Android.BankingTrojan.Mandrake	8.12
4	Android.MobileSpyware.mSpy	5.55
5	IoT.Bot.Mirai.variants	5.50
6	Android.MobileSpyware.MobileTracker	3.05
7	Android.InfoStealer.Multiverze	2.62
8	Win32.Bot.ZeroAccess2	2.58
9	OSX.Adware.AdLoad	1.99
10	Android.Trojan.SmsSpy.LA	1.98

Top attacks

Table 6 shows the top 10 attacks seen on mobile networks since the start of 2022. It includes attacks coming from mobile devices and also attacks coming from the internet. However, in many mobile networks, devices are issued with private IP addresses and use carrier-grade network address translation (NAT) to connect to the internet. In these cases, the devices are not visible from the internet and cannot be attacked directly.

Nearly two-thirds (60%) of attacks are associated with scanning for devices that allow SSH connections. These attacks don't actually do any damage on their own and, in most cases, have no impact on a user's mobile device. However, if the device does have an open SSH port, the attacker will then try to execute a brute-force login attack to gain access to the device and install additional malware, typically an IoT bot.

Table 6. Top 10 attacks in mobile networks, 2022-2023

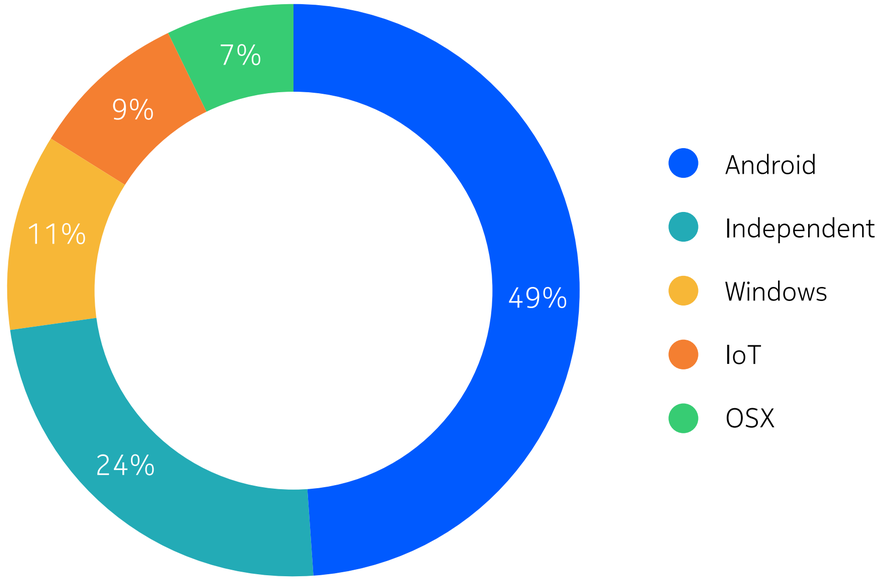
Rank	Malware name	%
1	Excessive SSH connection attempts	59.65
2	Host scanning for Cisco RV320 devices	32.03
3	Realtek RCE attempt (CVE-2021-35394)	1.14
4	SChannel possible heap overflow ECDSA with SHA-1 (CVE-2014-6321)	1.04
5	Suspicious quotation mark usage in FTP username	0.91
6	OpenSMTPD RCE attempt (CVE-2020-7247)	0.71
7	DNS amplification attack inbound	0.71
8	TCP SYN flood activity	0.57
9	ET IMAP Alt-N MDaemon IMAP server FETCH command buffer overflow	0.45
10	PHP Xdebug RCE attempt	0.20

Infections by device

Figure 7 provides a breakdown of the devices that have been most affected by malware in mobile networks.

Not surprisingly, Android-based systems continue to be the most targeted by mobile malware, accounting for nearly half (49%) of all infections. Approximately one-quarter (24%) of infections are from platform-independent malware, which could include smartphones, Windows, Linux and a variety of IoT devices. Windows infections (11%) are mostly from laptops and PCs tethered through a mobile phone, or accessing the network from a mobile Wi-Fi hotspot or directly via mobile dongle. This is also the case for OSX devices.

Figure 7. Mobile network malware infection by device, 2022-2023

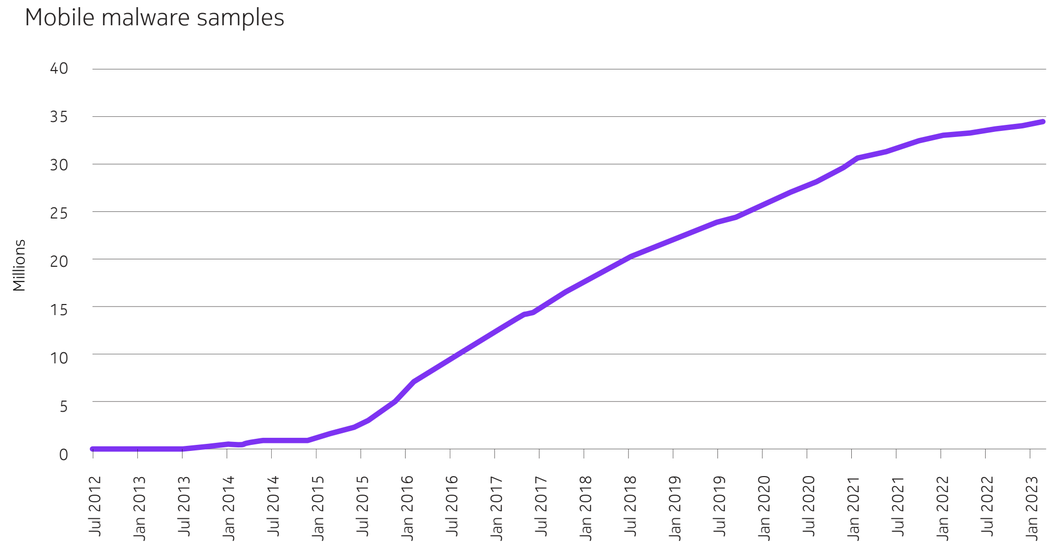


Android malware

Android based devices are not inherently insecure. However, most smartphone malware is distributed as trojanized applications and since Android users can load application from just about anywhere, it's much easier to trick them into installing applications that are infected with malware. Android users can protect themselves by only installing applications from secure app stores like Google Play and installing a mobile anti-virus product on their device.

Figure 8 shows the growth of Android malware samples collected by Nokia Threat Intelligence Center. Over the past two years, almost all of the malware has been distributed as trojanized applications.

Figure 8. Android malware samples, July 2012 – January 2023



Learnings and recommendations

Device visibility from the internet

The most common form of malware activity continues to be scanning for potentially vulnerable devices. It represents 88% of attacks in fixed networks and more than 90% in mobile networks. Once a vulnerable device is discovered, the malware launches a series of attacks to attempt to leverage the vulnerability, usually with the intent of adding the target device to a botnet.

In many mobile networks, devices are assigned private IP addresses and use carrier-grade NAT to access the internet, which protects them from being scanned from the internet. Similarly, in fixed broadband residential networks, usually only the home router has a public IP address. The devices in the home have private IP addresses and are not visible from the internet, protecting them from internet-based scanning and attacks.

Going forward, as IPv6 is more widely adopted, there will be no need to assign private IP addresses. All devices could potentially have public IPv6 addresses that are visible from the internet. However, this will remove the natural protection provided by NAT for home networks and many mobile devices. Being visible from the internet will mean these devices can be scanned and compromised. This problem can be addressed by making sure home routers and mobile gateways block inbound connections by default.

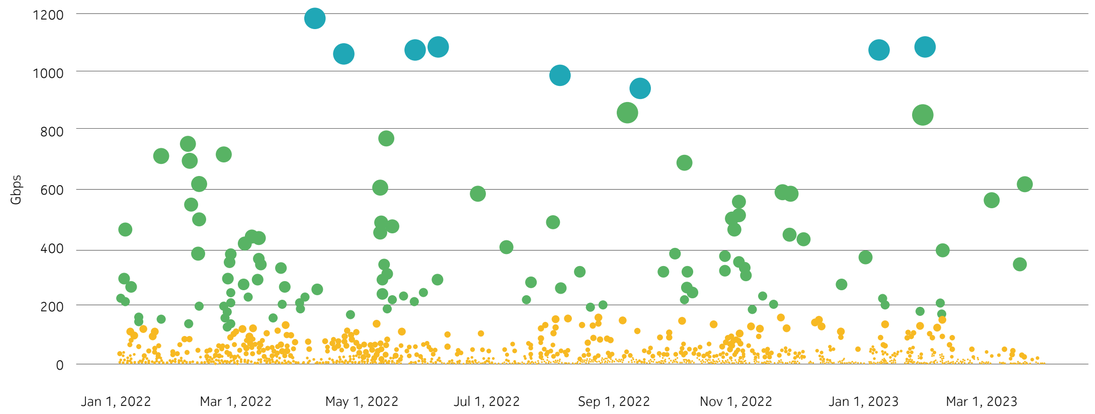
Trojanized applications

The most common way malware gets into a mobile device is for the device owner to be tricked into downloading and installing an app that contains malware. For Android users specifically, this risk can be somewhat mitigated by installing applications only from secure and trusted app stores, such as Google Play, and by installing an anti-virus product on their devices.

DDoS attack trends

In March 2023, Deepfield, a part of Nokia focusing on software applications for IP network analytics and DDoS security, conducted a study examining thousands of DDoS attacks recorded in 2022 and 2023. Figure 9 shows the number of attacks, their relative size and peak intensity during that period.

Figure 9. Distribution of DDoS attacks by peak intensity (Gbps), January 2022 – March 2023



This study found two major trends that mark a departure in how DDoS attacks have typically been done for the past 20 years:

- The emergence of botnets as the main sources of DDoS traffic.
- The "weaponization" of DDoS attacks, including signs of larger and more powerful botnets being co-opted into geopolitical conflicts.

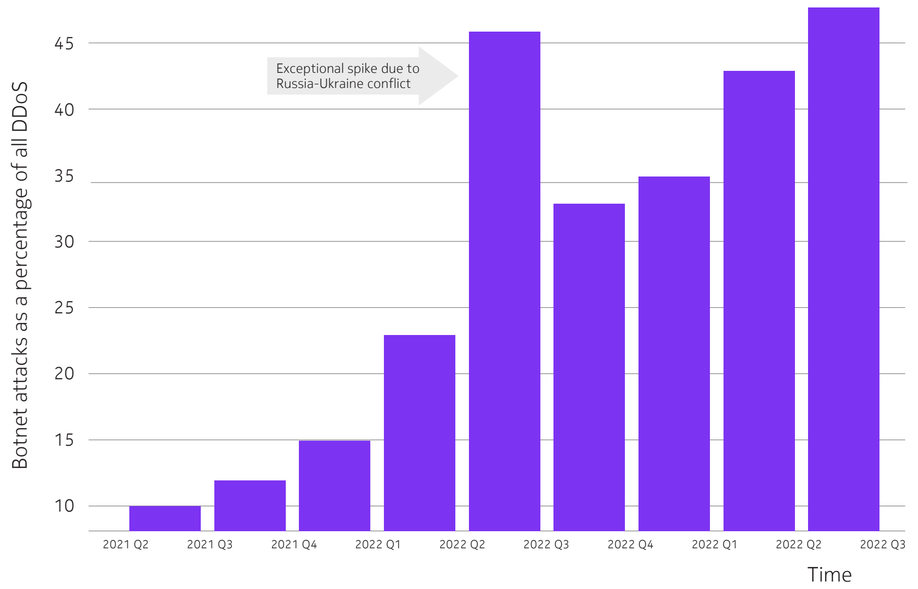
Botnets have taken over the (DDoS) world

Between 2000 and 2020, most DDoS attacks were based on spoofed traffic, using a variety of techniques (such as IP header modification) to hide the actual sources of the DDoS traffic. In a Nokia Deepfield study released in 2021, it was revealed that most DDoS traffic at that time was coming from fewer than 50 hosting companies and regional providers who were abusing open servers and hosts on the internet. That changed in 2022 and 2023, with botnets now generating most of the DDoS aggregate bandwidth (in bytes), as shown in Figure 10 — and representing the driving force in more than 90% of complex, multi-vector DDoS attacks.

The rise of IoT and cloud technologies in both residential and enterprise networks has contributed significantly to the expansion of botnets. DDoS bots are no longer limited to just home computers and routers — they now include remote monitoring and surveillance systems, digital video recorders, point-of-sale terminals, smart thermostats that control heating and cooling, devices used for remote data collection (e.g., water meters, parking meters), and even medical imaging systems in the healthcare industry. Even with 99% of enterprise IoT devices being secure, in a landscape of billions of connected devices, the remaining 1% that are vulnerable to compromise and exploitation represents a significant and growing threat.

Although the cloud is not the largest source (by number of devices), it is one the fastest growing in terms of bandwidth (in bits per second, or bps) and packet intensity (in packets per second, or pps), indicating the potential for even bigger and more impactful attacks in the future.

Figure 10. Botnet attacks as a percentage of all DDoS attacks, Q2 2021 – Q2 2023



Source: Nokia Deepfield

How big is the botnet DDoS danger?

Botnet DDoS traffic has exhibited significant growth over the past two years. In March 2023, we observed between 500,000 and 1,000,000 IoT hosts or cloud server instances engaged globally in regular daily DDoS activity — compared to about 200,000 in 2022. These large-scale botnets have a combined aggregate capacity between 50–100 Tbps, with most attacks across many networks worldwide showing 1–2 Tbps peaks.

That said, most attacks employ fewer than 5,000 devices but still have significant (sometimes devastating) effects on target systems and applications.

Today, DDoS attacks can come from inside (in many cases, from enterprise networks belonging to CSP customers) and outside of CSP networks (from the internet, across peering/transit links). Additionally, DDoS attacks can come from cloud providers even when CSPs have a direct link that may be treated as "clean" and hence not monitored. Because of the many new origination and entry points and directions of DDoS traffic, a more comprehensive, holistic approach to DDoS security is needed.

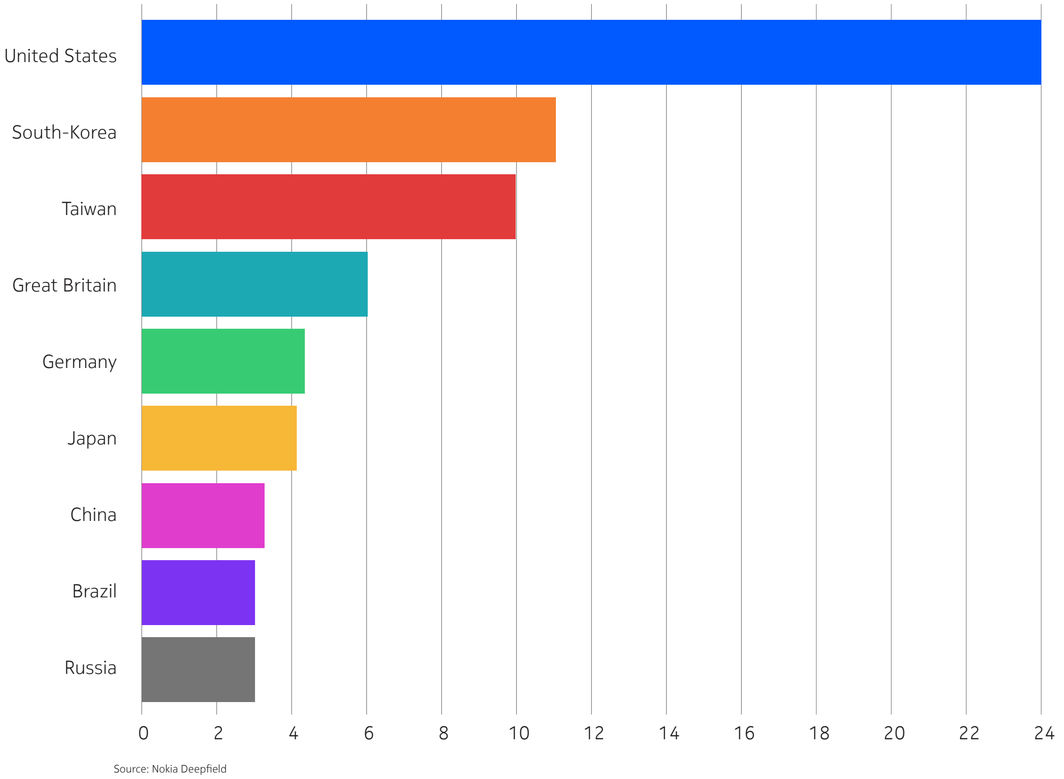
The geographical shift of the DDoS threat landscape

As shown in Figure 11, botnets are now a global issue, with active botnet devices no longer limited to specific geographies (such as Eastern Europe and Asia) as they were in the past.

Some threat actors are using this broad distribution of bot devices to launch truly global attacks, with some telecom networks witnessing attacks involving more than 60,000 active devices.

Still, at this point, the botnet threat is still somewhat limited: botnet-related DDoS bandwidth matches the DDoS bandwidth generated by all other attack types and varieties (e.g., amplification/ reflection, application DDoS). Also, more than 70% of all botnets use less than 50 Mbps per device. However, the race to gigabit speeds and symmetrical bandwidth is underway, increasing upstream capacity available with the adoption of PON, DOCSIS 4, 5G and FWA. This has the potential for individual bot speeds to reach more than 100 Mbps and multi-terabit levels for combined botnet attacks.

Figure 11. Geographical distribution of active botnet devices, by country



"Weaponization" of DDoS

Botnets are the source of tens of thousands of DDoS attacks daily, each involving anywhere between several thousand and several million IP addresses. These attacks can bring to a halt many CSP networks — and in doing so, disrupt communications, services and infrastructure across an entire country. For that reason, they have been used as a cyber weapon in the ongoing conflict between Russia and Ukraine.

Since the beginning of military operations in February 2022, the Nokia Deepfield research team has seen increased DDoS activity aimed at targets on both sides of the conflict. DDoS attacks have been aimed primarily at government sites, CSPs and banks. Some of this DDoS activity was short-lived (less than five minutes), meaning it was likely used as a diversion for other malware and intrusion attack vectors.

Initial DDoS attack vectors were mostly amplification/reflection and flooding, followed by HTTP/DNS attacks. Additional attack vectors were added and combined, mostly employing botnet and amplification/ reflection attacks from sources located in other non-neighboring countries. Consequently, some CSPs noticed increased upstream traffic to their peering and transit partners — in some cases, up to the point of noticeable degradation of downstream services.

For several CSPs, the fact that devices in their networks (and from their customers) can be co-opted to participate in a conflict that is geographically constrained — but without limits in cyberspace — was a sign to start looking into new DDoS security solutions or multi-layer security models.

Learnings and recommendations

Detecting botnet DDoS traffic is challenging because traditional approaches to detection, such as thresholds or baselines, are not effective. Botnet traffic circumvents traditional anti-DDoS systems as it appears to be real — that is, it comes from real devices and exhibits characteristics of real traffic. The challenge is to be better at accurately detecting botnet DDoS activity and lowering the rate of false positives so legitimate customer traffic is not altered or disrupted.

For more than 95% of DDoS attacks, defense is no longer about looking at what's inside the packet. Instead, it's about who/what is sending the packets — and better understanding the larger internet security context. Additionally, while CSPs have traditionally been guarding only the front door (i.e., peering/ transit links), attacks now come from many other entry points, including their customers, partners (e.g., cloud providers) and even compromised devices in their own networks. Legacy-based solutions do not adequately monitor DDoS traffic originating from these new entry points.

An approach driven by big data analytics that correlates network traffic in real time with a broader internet context (e.g., which type of device is behind a source IP address), when combined with the programmability of the latest generation of IP network routers, is much more effective in detecting botnet DDoS activity (and with fewer false positives). It also enables more agile and granular network-based mitigation. Additionally, the progress of artificial intelligence and machine learning has resulted in the development of security models that can be trained on real-world data to result in even more advanced DDoS detection and mitigation.

Over the last few years, we have seen great examples of digital cooperation between telecom service providers, cloud providers, regulators and governments to grow, connect and secure network infrastructures worldwide. That is why we created the **Nokia Deepfield Global DDoS Threat Alliance (GDTA)**: an opt-in, membership-based organization that allows Nokia customers to share information about DDoS activity — and by doing so, better protect themselves against current, new and emerging DDoS threats.

Security Intelligence and Operations Center trends

Experts at Nokia Security Intelligence and Operations Centers (SIOC) observe hundreds of security incidents each month, while our NetGuard Endpoint Detection Response (EDR) team observes hundreds of incidents every six months. This section of the report describes the security trends they are seeing.

Critical incidents

Access abuse

Access abuse is when users misuse or exploit legitimate permissions for malicious purposes. When directed against a business, they can negatively affect the functions that bring in revenue or provide a positive user experience — for example, by causing network outages and service disruptions. They can also lead to regulatory compliance issues.

Some of the access abuse incidents observed by Nokia's SIOC team include:

- **Execution of critical commands outside of a maintenance window** (on average, two incidents every day)
- **Login to a critical device in a non-maintenance window** (on average, 20 incidents each month)
- **Unauthorized access of personally identifiable information (PII) files** (on average, one incident per month)

Privilege escalation

Privilege escalation is when a user deliberately raises their level of permissions to get more access rights. Over a six-month period, our EDR team found that privilege escalations accounted for 35% of all incidents observed.

One example is the PwnKit exploit, which allows unprivileged users to gain root privileges on an affected system even in its default configuration. This can result in full account takeover and account compromise.

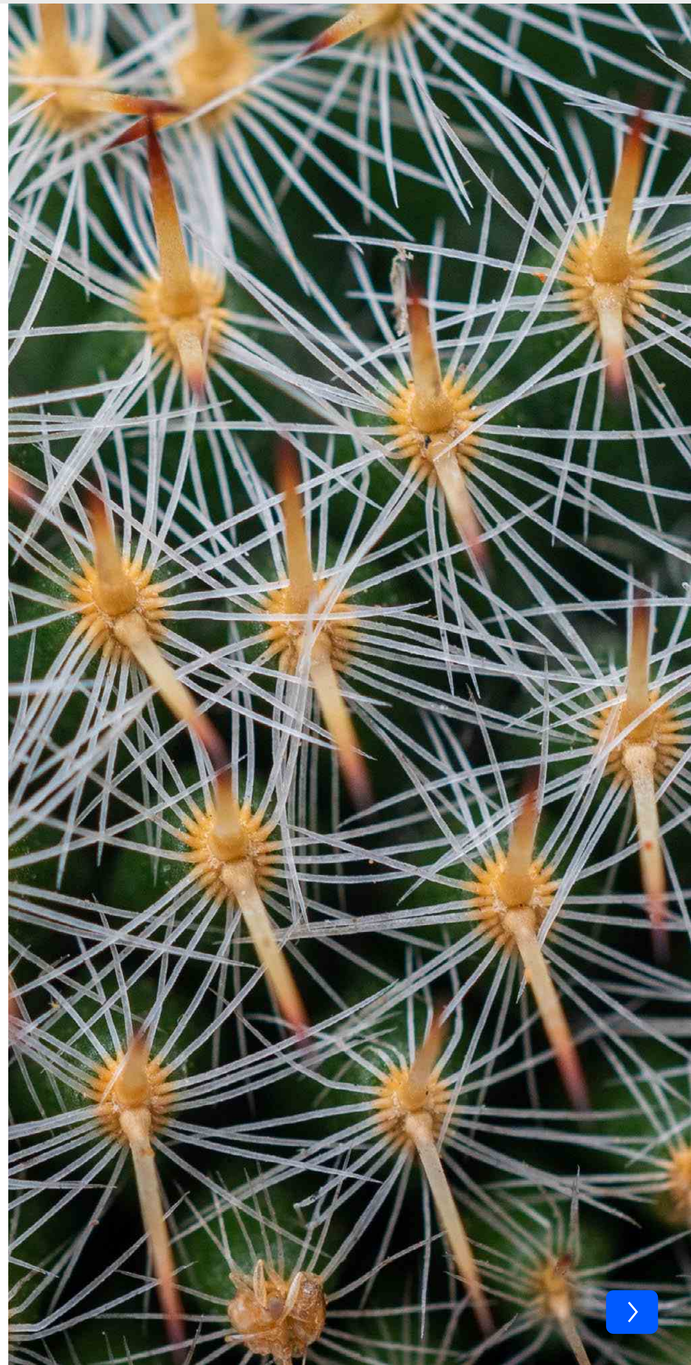
Malicious probes

Malicious probes, also known as network probes, refer to unauthorized attempts to access or gather information from a network or system with malicious intent. They can take various forms, such as port scanning, which involves scanning a network to identify open ports that may indicate potential vulnerabilities.

Of the malicious probe incidents observed in our SIOC, 90% were launched with the intent to lead to a DDoS attack, resource exhaustion or malware upload.

Malware and backdoor attacks

Our EDR team found that, over a six-month period, 33% of all observed incidents were backdoor and malware attacks. These included the TSUNAMI IRC botnet, TinyShell incidents, Linux backdoor incidents and Mimikatz exploitation.

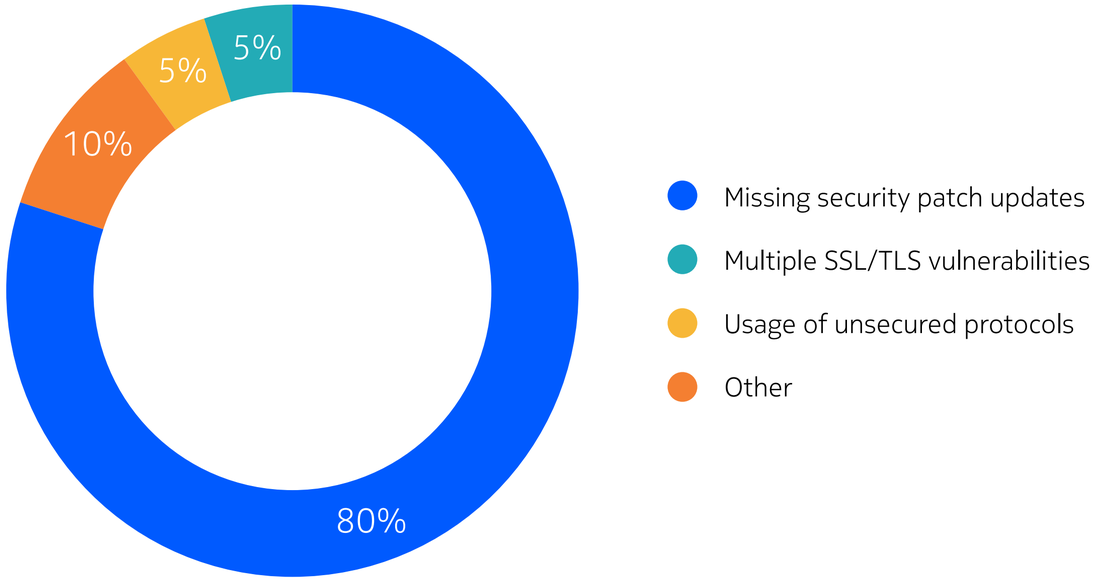


Vulnerability assessment and penetration testing

Every quarter, our network vulnerability assessment and penetration testing (VAPT) experts perform an average of more than 100 scans. Some of the critical and high vulnerabilities identified include:

- **Using unsecured protocols:** We have observed the use of unsecured protocols such as FTP and HTTP, which can lead to "man-in-the-middle" attacks, unauthorized access and regulatory compliance concerns.
- **Protocol misconfiguration:** We have observed multiple protocol misconfiguration vulnerabilities, including the use of weak versions of SSL and TLS (SSL v2, SSL v3, TLS v1.0, TLS v1.1), as well as the use of weak ciphers and signatures. Misconfigured protocols can enable attacks such as POODLE and Heartbleed.
- **Missing security patch updates:** The majority of the vulnerabilities we have observed are due to missing security patch updates. When mandatory patches are not applied, this can have several negative impacts on the security and integrity of software, systems and networks, including vulnerability exploitation, malware infection and an increased attack surface.

Figure 12. Vulnerabilities detected by vulnerability assessment and penetration testing



Telecom interface security assessment

Critical and high security trends identified by our telecom security specialists include:

Diameter attacks via S6a ULR: The Diameter protocol is associated with many of the most common security vulnerabilities, including denial-of-service (DoS) attacks, spoofing, message tampering, information leakage and replay attacks. One such tactic leverages S6a ULR (update location request) messages, an important communication protocol used in telecom networks to inform the home subscriber server (HSS) about changes made by a subscriber in the serving mobility management entity (MME) and to request profile data. The S6a ULR message can be exploited by attackers to carry out SMS interception, DoS attacks and subscriber profile disclosure. Unfortunately, many telecom networks lack adequate security measures or have implemented them incorrectly, making it easy for attackers to exploit these legacy vulnerabilities and commit identity theft and financial fraud.

Diameter attacks via S6a RSR: There is also the S6a RSR (restart request) message, which is used by the HSS to inform the MME about the need to restart the ULR procedure for a specified group of subscribers. If the HSS is exploited to send an RSR message that involves thousands of even millions of International Mobile Subscriber Identities (IMSIs), it can cause a significant amount of message flow in the network — resulting in an overload of both the MME and HSS, causing performance issues or even system crashes. Again, many telecom networks lack adequate security measures to stop this exploit or have not implemented them incorrectly.

GTP attacks: GPRS Tunnelling Protocol (GTP) is used in mobile networks for transferring user data packets between different network nodes. However, it can also be used maliciously by attackers to gain unauthorized access to the internet at the expense of others. For example, an attacker can exploit vulnerabilities in the GTP to bypass billing systems and use someone else's data plan to access the internet, which could lead to unauthorized charges for the victim and potentially cause financial losses.

USSD fraud via SS7: Unstructured Supplementary Service Data (USSD) is a communication protocol used for sending and receiving text messages between a mobile device and a service provider. An attacker can exploit Signaling System 7 (SS7) to intercept USSD messages and manipulate them to execute unauthorized transactions on a victim's mobile device. They can also use SS7 to launch DoS attacks by flooding the network with SS7 packets, disrupting network services for legitimate users. We have seen that attackers can easily target a CSP's subscribers to commit USSD fraud due to improper placement of security measures in telecom networks.

RAN/air interface attacks: The RAN/air interface is a crucial component of mobile networks, enabling wireless communication between mobile devices and network infrastructure. However, it is vulnerable to attacks such as rogue enhanced NodeB (eNB) latching and IMSI catching, largely because radio access networks are kept at a low priority for security implementation. With rogue eNB latching, an attacker can set up a fake eNB that is not authorized by the network operator but appears to be legitimate. That eNB can then attach to the operator's core network, potentially enabling the attacker to intercept and manipulate network traffic or launch other types of attacks. With IMSI catching, an attacker can use specialized equipment (either a standalone eNB or a rogue eNB attached to the core network) to intercept and collect IMSI information from mobile devices as they communicate with the network.

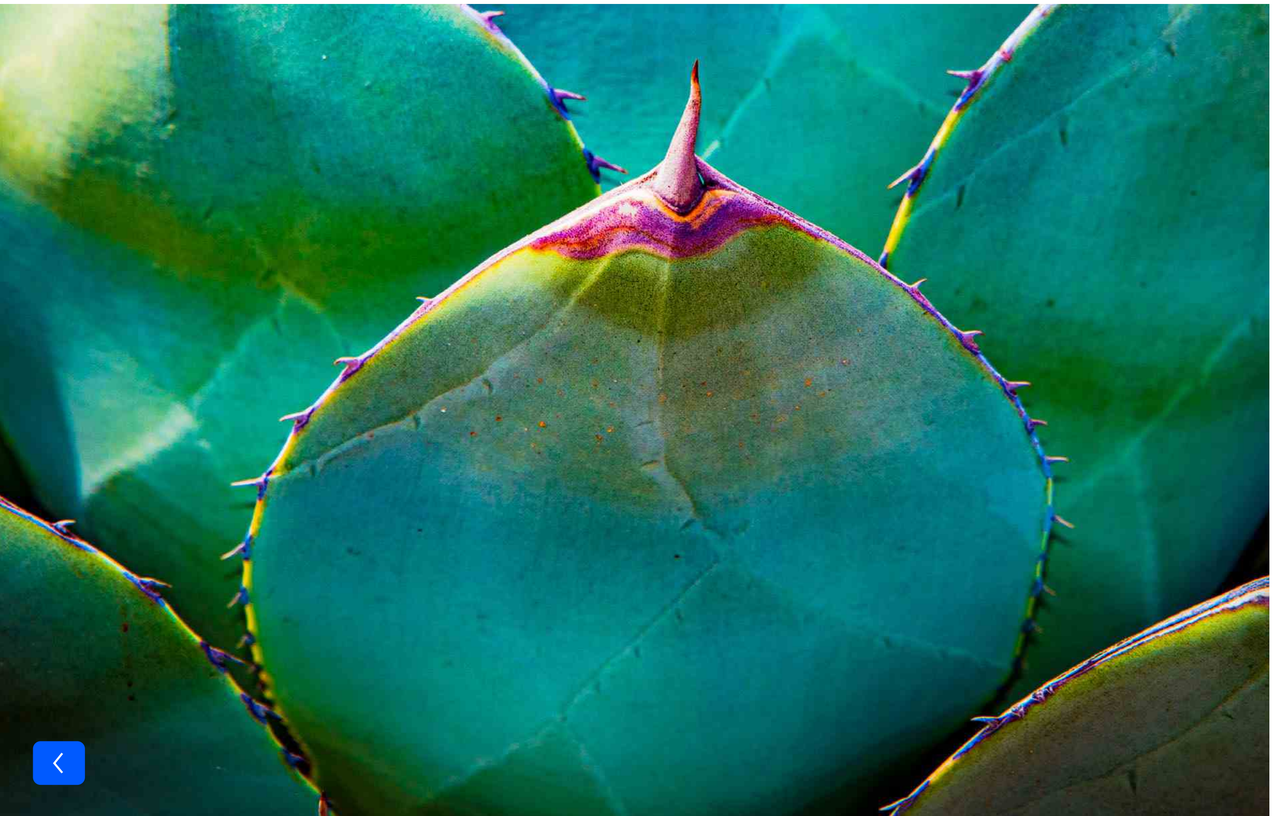
VoLTE/VoWi-Fi attacks: Due to the legacy architecture of VoIP networks, VoLTE/VoWi-Fi networks are susceptible to a serious security issue. Specifically, we have observed that these networks can allow two or more devices to communicate with each other directly, creating an opportunity for attackers to exploit the situation. For example, attackers can leverage open-source tools to root mobile devices or use SIM card readers to establish a direct tunnel between their computers and the IP Multimedia Subsystem (IMS). By doing so, they can bypass billing systems and lawful interception mechanisms that are in place. Because the communication occurs through a direct tunnel, it may not be detected by the network operator or other security mechanisms.

Fixed line and broadband hijacking: By taking control of a subscriber's optical network terminal (ONT) or customer-premises equipment (CPE), an attacker can intercept and manipulate the subscriber's internet traffic, potentially compromising sensitive information or using the internet connection for malicious purposes. Also, due to the flat network architecture in most legacy telecom networks, the attacker may also be able to bypass the security and lawful interception mechanisms implemented by the internet service provider (ISP) and gain access to the ISP's infrastructure, further expanding their attack surface.

Fixed line and broadband SIP credential stealing: CPE/ONT devices often use encryption to secure the data of SIP authentication and authorization at CWPM servers. We have seen that it is possible to exploit vulnerabilities in the encryption algorithms to break the encryption and steal the authentication credentials, enabling unauthorized access to the subscriber's voice and data services. Using the stolen SIP authentication credential, it is also possible to conduct billing frauds or, due to outdated VoIP system architecture and lack of security measures in CPEs, impersonate MSISDN and IP addresses.

CSP perspectives on security threats

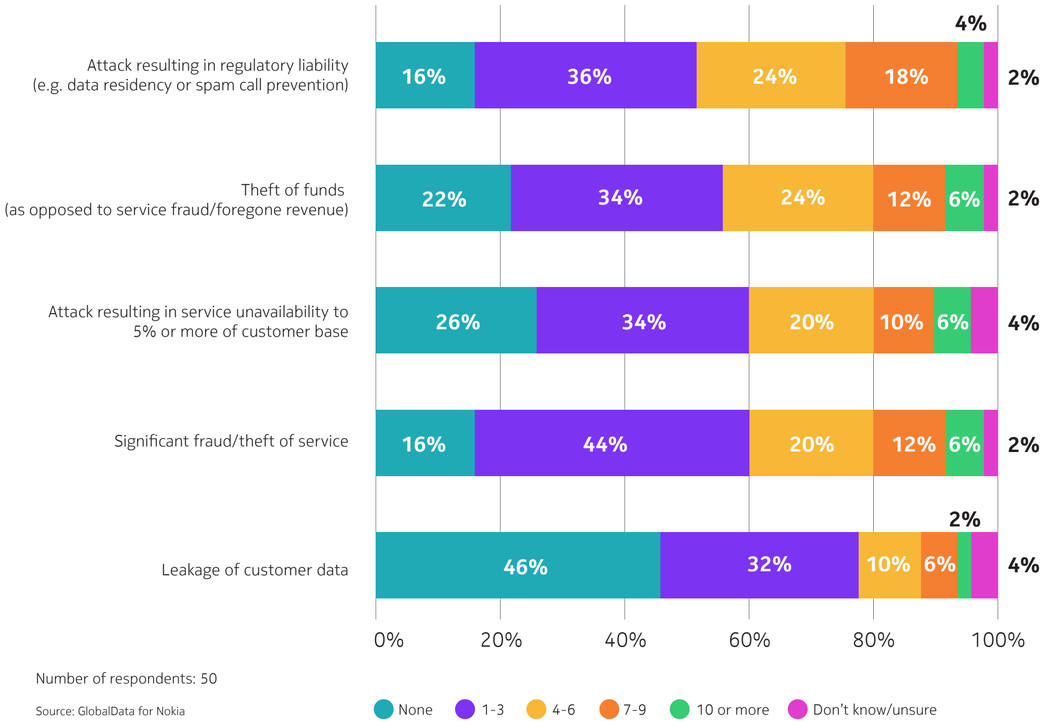
In 2022, Nokia commissioned GlobalData to conduct research into the 5G security landscape and the managed security services market. Online surveys and in-depth interviews were conducted with 50 CSPs around the world. The following is a recap of the main findings related to cyber threats from the final research report.



Breaches are the rule, not the exception

The overwhelming majority of CSPs experienced at least one breach in the last 12 months, with at least one-third of respondents reporting eight or more breaches in a single attack category, as shown in Figure 13.

Figure 13. Number of breaches by type in the last 12 months



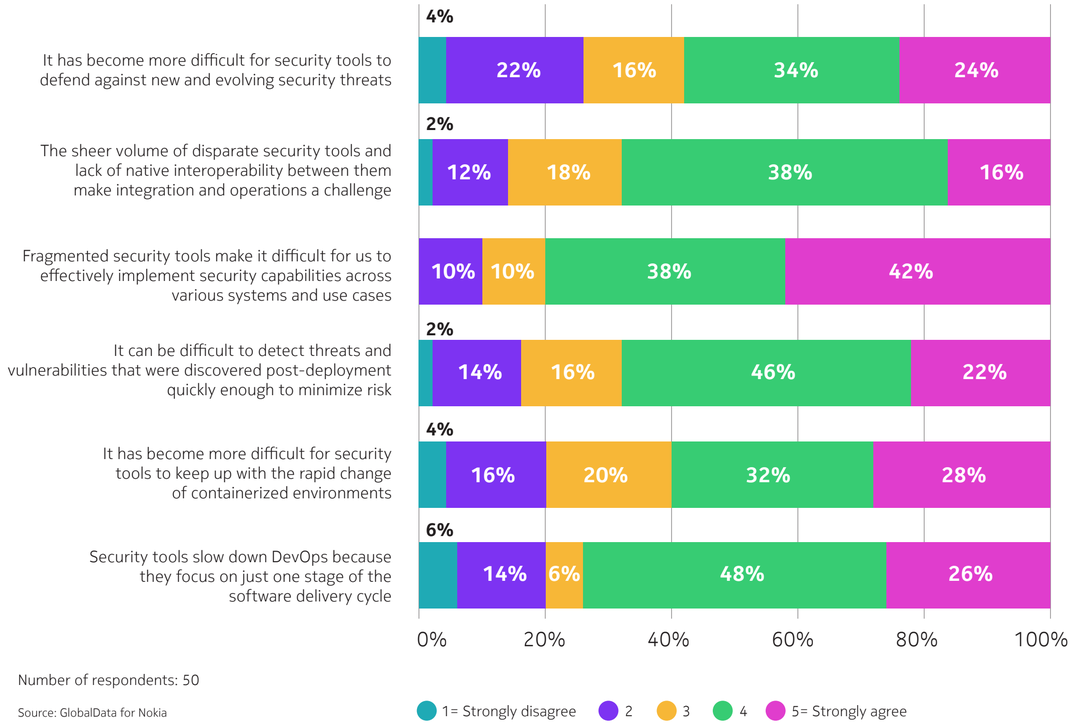
Number of respondents: 50

Source: GlobalData for Nokia

Fragmentation of security tools is a huge issue

As shown in Figure 14, when asked about the main security challenges they face, the vast majority of CSPs said fragmented tools are making it difficult to effectively implement security capabilities across various systems and use cases.

Figure 14. Main challenges with existing security tools and approaches



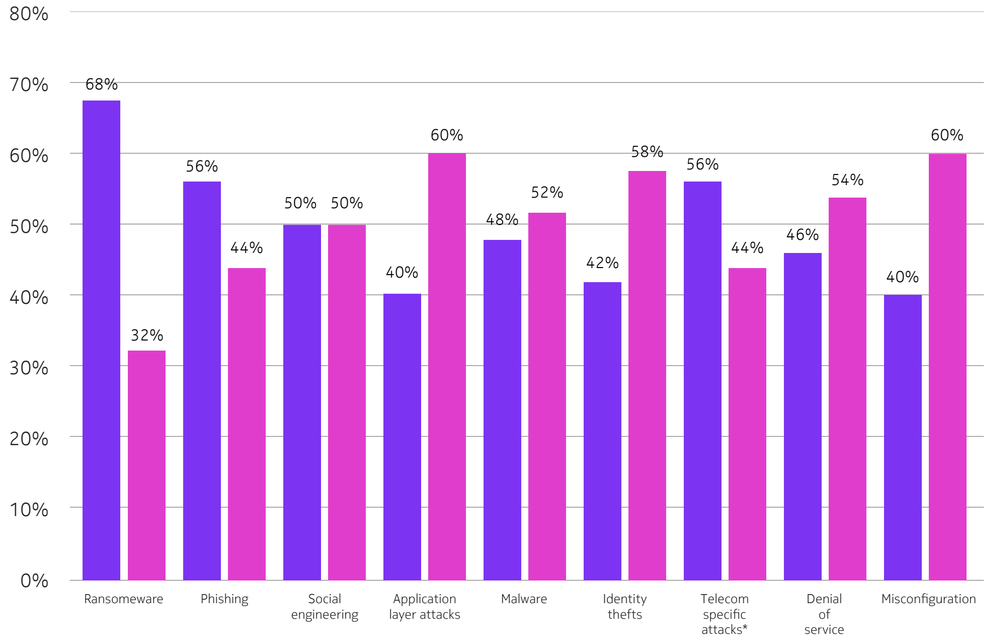
Number of respondents: 50

Source: GlobalData for Nokia

CSPs are looking to improve the security of their 5G operations

As shown in Figure 15, when asked about the areas in which they need to substantially improve their security capabilities for 5G, more than two-thirds of CSPs cited ransomware, followed by telecom-specific attacks (such as call redirection/interception), phishing and social engineering attacks.

Figure 15. Areas where CSPs need to improve security capabilities for 5G operations



Number of respondents: 50

Source: GlobalData for Nokia

*Like illegal call redirection, interception, messaging attacks, etc.

Findings based on Nokia's interactions with CSPs

Our security experts regularly engage with CSPs to discuss the security aspects of telecom networks. The top security-related concerns mentioned during these interactions include the following:

Regulatory compliance and reporting

All over the world, cybersecurity regulations are becoming increasingly stringent. As such, CSPs are looking to become more agile so they can quickly share reports to government agencies to prove compliance, when asked.

In addition, CSPs and regulators alike are increasingly seeking service-level agreements that specify time-bound mitigation of vulnerabilities identified in the network elements supplied by their vendors. This is being driven primarily by regulators that expect such guarantees from the CSPs and other entities that manage critical infrastructure, which, in turn, get pushed by the CSPs onto their vendors. Compliance with Center for Internet Security (CIS) benchmarks is also highly sought after by CSPs as an assurance that the products supplied by their vendors are securely hardened.

Endpoint detection and response

As governments establish new regulations and requirements for cybersecurity that affect mobile core networks, this is creating the need for EDR capabilities in the core network elements.

An EDR solution works by providing real-time visibility into endpoint activities. This is achieved by deploying a software agent onto a monitored host. In the telecom context, this might be a virtual network function (VNF) or a server with Kubernetes-based cloud-native network functions (CNFs).

As it relates to EDR, CSPs have the following concerns:

- Most enterprise EDR solutions depend on centralized services hosted on the public cloud. This requires data to be shared outside of the CSP's network and sometimes to data centers outside of the CSP's country. This dependency on a centralized service will also often overlap with the CSP's existing security ecosystem.
- Installing any third-party EDR agents in mission-critical 5G core networks elements can bring risks to the capacity, performance and stability of those elements. In turn, this can affect a CSP's service-level agreements.
- Addressing vulnerabilities with an IT-based EDR system can create critical vulnerabilities on telco infrastructure and applications. These include a dependency on having root privileges, access to kernel space, the need to disable certain built-in protection mechanisms of the network functions, changes to IP communication settings and exposure of sensitive personal data processed by the network functions.

Because CSPs want to ensure continuous monitoring of their infrastructure at all levels, they are demanding compatibility of security products with different EDR agents currently on the market.

Geopolitical considerations

A more recent trend is the need for CSPs to mitigate risks related to geopolitical developments, including:

- **Bills of material notification:** A software bill of material (a list of all the open-source and third-party components used in software) is increasingly becoming a mandatory requirement for selling products in some countries.
- **Supply chain country exclusion:** Many countries are listing requirements for excluding specific countries from the supply chain of telecom product vendors.
- **Human resource and data localization:** As deglobalization increases, there are greater demands related to the localization of data and labor.
- **Product security assurance:** Because their vendors can come from many different countries, CSPs are increasingly expecting assurance of the security posture of the products they receive from their vendors (e.g., through security certifications or specially curated test reports).
- **Personnel security clearance:** CSPs are increasingly seeking security clearances from the vendor personnel accessing their networks.

Conclusion

In 2022, the majority of attacks on telecom mobile networks were linked to IoT bots that scan the network for vulnerable hosts, looking to add new devices to their botnets for use in DDoS attacks. Thanks to the rise of IoT and cloud technologies in both residential and enterprise networks, botnets have expanded at a considerable rate — and have become a major generator of DDoS traffic. As of 2023, about 90% of all complex, multi-vector DDoS attacks are now based on botnets. In addition, we are seeing between 500,000 and 1,000,000 globally distributed, remotely controlled IoT hosts or cloud server instances active on a daily basis, generating more than 40% of all DDoS traffic. There are also signs that DDoS is becoming increasingly weaponized, with larger and more powerful botnets being co-opted into geopolitical conflicts.

The most common malware attacks are ad-click bots, crypto-miners and banking trojans. While adware decreased by 25% from 2021 to 2023, crypto-mining kept stable and banking trojans almost doubled, climbing from 5% to 9% of all attacks detected. Overall, there was a steady decline in residential malware infection rates, which fell from 3% to 1.5%. This is largely because more and more people are returning to office work environments post-pandemic, so malware campaigns targeting remote workers have tapered off. However, infection rates have not yet returned to their pre-pandemic level of 1%.

Globally, as cybersecurity regulations become more stringent, CSPs are striving to become more agile so they can quickly share reports with government agencies to prove compliance. But many CSPs are struggling to keep pace with the latest threats, with more than 30% experiencing eight or more security breaches in the last 12 months. As technology continues to advance, so are the tactics and techniques being used by cyber attackers. CSPs must continue to be cautious of the top predicted threats — ransomware, IoT device vulnerability, insider threats, supply chain attacks — and consider how best to prepare for and mitigate these risks.

The introduction of 5G is enabling the use of more and more IoT devices, which is further opening up the attack surface available to threat actors. 5G also makes possible multi-access edge computing (MEC), which will pose a new challenge of securely managing multi-vendor applications at the network edge.

By staying informed of the latest attack trends and implementing effective security strategies, CSPs can protect their networks and safeguard their customers' data. At Nokia, we recommend CSPs use a cyber threat intelligence framework that focuses on attack phases, tactical objectives and techniques used by adversaries. This kind of framework will provide a comprehensive view of the nature of the threats CSPs face as well as more meaningful information about adversary behavior — and how to respond appropriately.

About Nokia's security capabilities

Nokia offers a broad range of security products and services to help CSPs identify threats quickly, stop them automatically and take fast remediation actions when needed — so they can protect their networks from degradation and deliver on their service-level agreements.

For more information on Nokia security portfolio, visit:

www.nokia.com/networks/security-portfolio

Nokia Threat Intelligence Center examines malware network communications to develop detection rules that identify malware infections based on command-and-control communication and other network behavior. These rules enable the fast detection of malware in CSP networks.

For more information on the Nokia Threat Intelligence Center, visit:

www.nokia.com/networks/security-portfolio/threat-intelligence

Nokia DDoS detection and mitigation solution, centered around Deepfield Defender, combines big data analytics, the detailed internet security context from our patented Deepfield Secure Genome™ data feed and the programmability of the latest generations of FP4/FP5-based Nokia service routers to provides 360-degree protection against both inbound (external, from the internet) and outbound (internal, from hijacked or malicious devices within a CSP's network) threats and attacks.

For more information on the Nokia DDoS security solution, visit:

www.nokia.com/networks/ip-networks/deepfield/defender/

Nokia Security Intelligence and Operations Center manages the security of multiple telecom networks 24/7 to prevent and stop threats before they materialize. Its comprehensive view into the latest trends on critical security incidents, application security, and vulnerability assessment and penetration testing is based on observed activity across networks worldwide.

For more information on Nokia Managed Security Services, visit:

www.nokia.com/networks/services/managed-security-services

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 213316

nokia.com

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.