Threat Intelligence Report 2020

This report provides a view of malware activity in mobile and fixed networks around the world. The data in this report has been aggregated from service provider networks where Nokia's NetGuard Endpoint Security solution is deployed. This network-based malware detection solution enables Nokia customers to monitor their fixed and mobile networks for evidence of malware infections in consumer and enterprise endpoint devices, including mobile phones, laptops, personal computers, notepads and the new generation of Internet of Things (IoT) devices. This solution is deployed in major fixed and mobile networks around the world, monitoring network traffic from more than 150 million devices.

The system examines network traffic for malware command-and-control communication, exploit attempts, hacking activity, scanning activity and Distributed Denial of Service (DDoS) attacks. This enables the system to accurately determine which devices are infected with malware and what malware is involved. The system also monitors attack traffic to determine where the attacks are coming from and what network devices are being attacked.

The report also includes details from malware analysis conducted in the sandbox environments in our malware analysis lab and additional information from our honeypot systems.

Main findings

Covid-19 caused a surge in mobile malware infections.

In 2020, the average monthly infection rate in mobile networks was 0.23%. In February and March, however, the monthly mobile infection rate increased by almost 30% over the previous months, largely due to the significant escalation of cyber security incidents related to the Covid-19 pandemic.

The impact of Covid-19 was felt later in fixed broadband.

For fixed broadband networks, the average monthly infection rate per residence was 2.16%. While this is down overall compared to 2019, there was a sharp increase in infection rates in May and June due to the Covid-19 pandemic — but this spike happened two months after the one observed in mobile networks.

Infections have increased significantly in the IoT space.

IoT devices are now responsible for 32.72% of all infections observed in mobile networks, up from 16.17% in 2019. This trend lines up with the growing number of IoT devices that are now connected to mobile networks. Nokia's Threat Intelligence Lab anticipated this trend and has monitored the situation closely throughout the year.

Android devices are the most common malware targets.

Android devices are responsible for 26.64% of infections across all platforms, but this is down from 47.15% in 2019. While this change is due in part to improved security in Android device, it is mostly the result of the increase in IoT-related infections.

PCs lead the way in infections.

Windows/PCs are responsible for 38.92% of all infections, up slightly from 35.82% in 2019.

Info-stealers and spyware are on the rise.

There is a strong trend toward info-stealers and mobile spyware, which make up 35.76% of all Android infections.

Trojans are now the malware of choice.

The share of malware detected as Trojans jumped to 74% from just 34% in 2019, largely because the exceptional circumstance of this year have made phishing campaigns the best way to delivery malware directly to users. The relative share of worms and viruses has decreased in 2020.

Covid-19 pandemic scare exploited by cyber criminals

The Covid-19 pandemic has wide social and economic implications in countries around the globe. As expected, cybercriminals are playing on people's fears and are seeing this situation as an opportunity to promote their agendas.

Nokia's Threat Intelligence Lab is monitoring the situation and providing actionable threat intelligence to detect Covid-19 malware variants as well as established malware delivered through Coronavirus-related phishing campaigns.

Covid-19 specific malware

Some of the malware observed in mobile and fixed networks has been created specifically for the occasion. They were mostly created hastily and are not very sophisticated, but are nonetheless effective, as users became more susceptible to the tricks used by the attackers

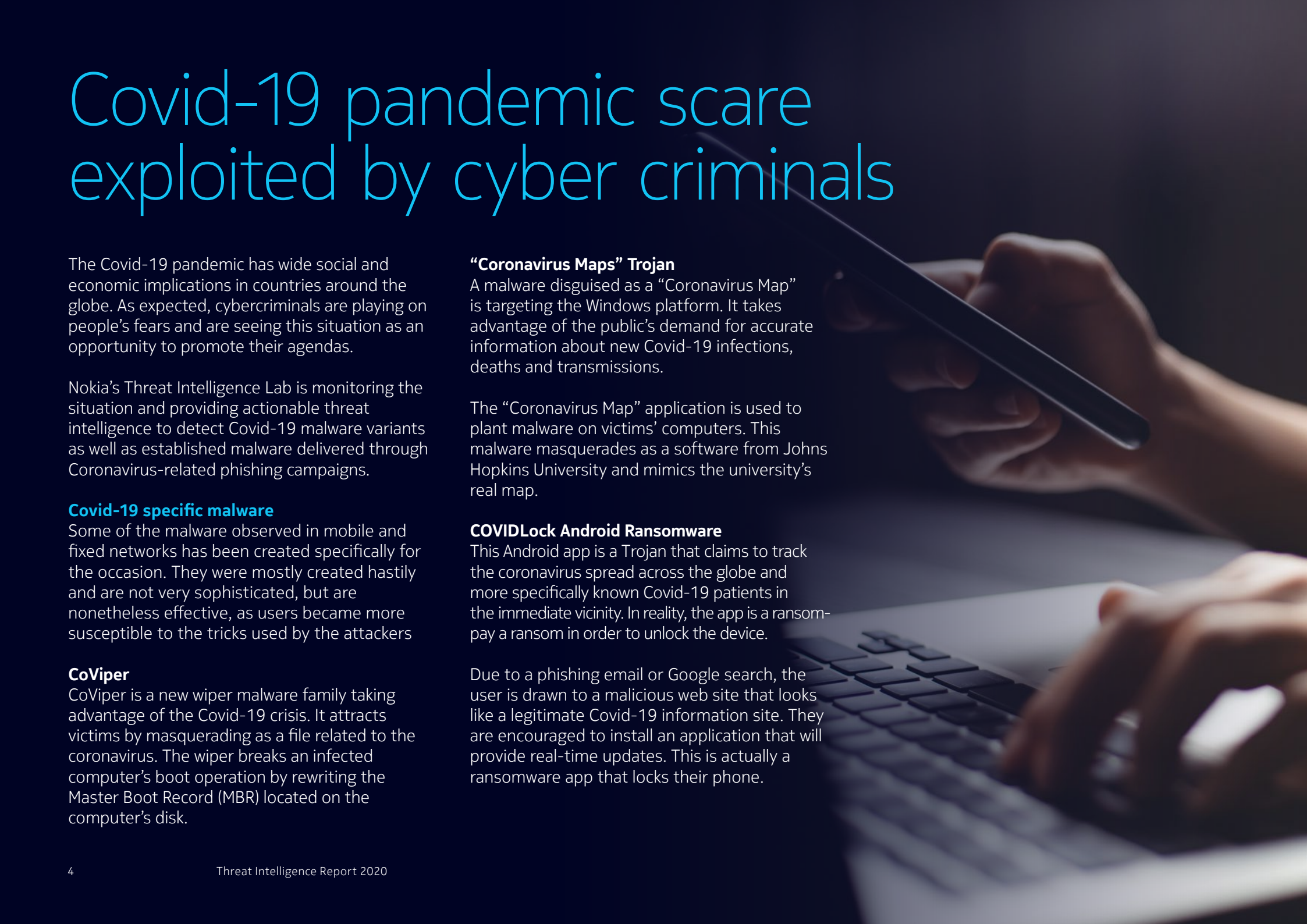
CoViper
CoViper is a new wiper malware family taking advantage of the Covid-19 crisis. It attracts victims by masquerading as a file related to the coronavirus. The wiper breaks an infected computer's boot operation by rewriting the Master Boot Record (MBR) located on the computer's disk.

"Coronavirus Maps" Trojan
A malware disguised as a "Coronavirus Map" is targeting the Windows platform. It takes advantage of the public's demand for accurate information about new Covid-19 infections, deaths and transmissions.

The "Coronavirus Map" application is used to plant malware on victims' computers. This malware masquerades as a software from Johns Hopkins University and mimics the university's real map.

COVIDLock Android Ransomware
This Android app is a Trojan that claims to track the coronavirus spread across the globe and more specifically known Covid-19 patients in the immediate vicinity. In reality, the app is a ransom-pay a ransom in order to unlock the device.

Due to a phishing email or Google search, the user is drawn to a malicious web site that looks like a legitimate Covid-19 information site. They are encouraged to install an application that will provide real-time updates. This is actually a ransomware app that locks their phone.



COVID-19 themed phishing attacks delivering various malwares

In addition to malware that was specifically created or modified to fit the Covid-19 theme, some phishing campaigns are tailored to this theme but are delivering existing malware. Below is a list of observed phishing campaigns that exploit the sense of urgency around Covid-19.

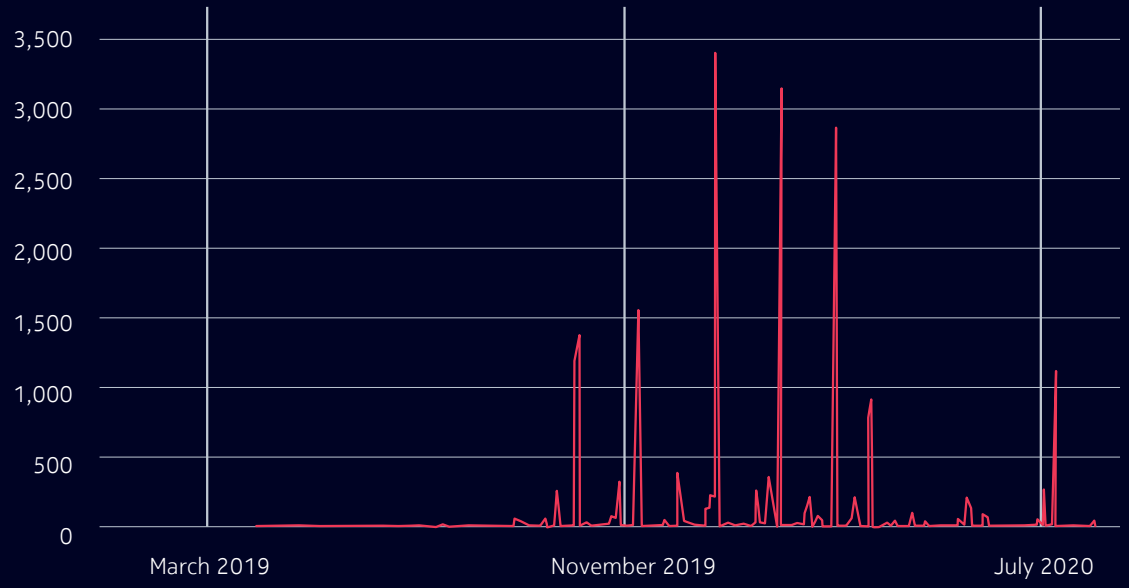
Remcos RAT

Remcos is a sophisticated remote access Trojan (RAT) that can be used to fully control and monitor any Windows computer from XP onwards. It is widely used in multiple malicious campaigns by threat actors.

The latest campaign utilizes social engineering technique wherein threat actors are leveraging what's new and trending worldwide. The phishing email contains a PDF offering coronavirus safety measures, but in reality this PDF includes executable for a REMCOS RAT dropper that runs together with a VBS file executing the malware.

As illustrated in Figure 1, versions of the malware that were used in previous campaigns are reused in the Covid-19 campaigns. For this particular version of the malware, Win32.Backdoor.Remcosrat.A, the peak was reached at the end of the year, but it got a new life as it was reused in the COVID-19 campaign in July 2020.

Figure 1. Win32.Backdoor.Remcosrat.A – Daily Infection Rate



Plugx delivered by Covid-19 themed documents

PlugX a malicious program that targets the Windows platform. This malware is usually distributed through phishing emails, infected websites and malicious software. Its primary goal is to drop malicious payload. After the malware has established persistence on a system, it tries to establish a network connection with the Command and Control server.

PlugX sends sensitive information of the device to the C&C server, deletes or changes registry entries and changes plugins as directed by the C&C server.

HawkEye info-stealer distributed as fake Covid-19 drug advice

A new HawkEye malware variant is being distributed in mails spoofing the World Health Organization. The email appears to be sent directly from Dr. Tedros Adhanom Ghebreyesus, Director-General, World Health Organization (WHO).

HawkEye is a malicious information-stealing malware that targets the Windows operating system. The malware is delivered via spam emails containing malicious URL links or macro embedded files. Once installed, the malware steals sensitive information using the technique of browser key-logging. The malware is also able to download additional malware to the compromised system.

Kimsuky Covid-19 campaign
Kimsuky malware is delivered as a Microsoft Word file masquerading as information about the Covid-19 pandemic. The document contains a macro that will execute should the user fall for the request to enable additional content downloads to properly view the document. When opened, the malicious macro connects with Command and Control and tries to retrieve a file from site.

Android.Corona Safety Mask SMS Scam
COVIDSafetyMask is a malicious info-stealer that targets Android devices. This program masquerades as an application to help users get safety masks. Upon infection, it will ask permission for contacts and SMS messages.

Once it gains permission required, the malware will send fraudulent messages to victims' contacts in order to spread itself.

Android. "corona live 1.1" SpyMax surveillance-ware
"corona live 1.1" is a Trojanized version of a legitimate coronavirus tracking application for Android devices. It is part of the SpyMax surveillance-ware family and has all of the capabilities contained within SpyMax such as a call manager, SMS manager, camera manager. It provides the malicious actor with access to sensitive data on the phone and allows the attacker to remotely activate the camera and the microphone.

Anubis, Cerberus, Gimp
These are some of the numerous other older malwares that were seen being distributed in the context of Covid-19 phishing campaigns.

Recommendations

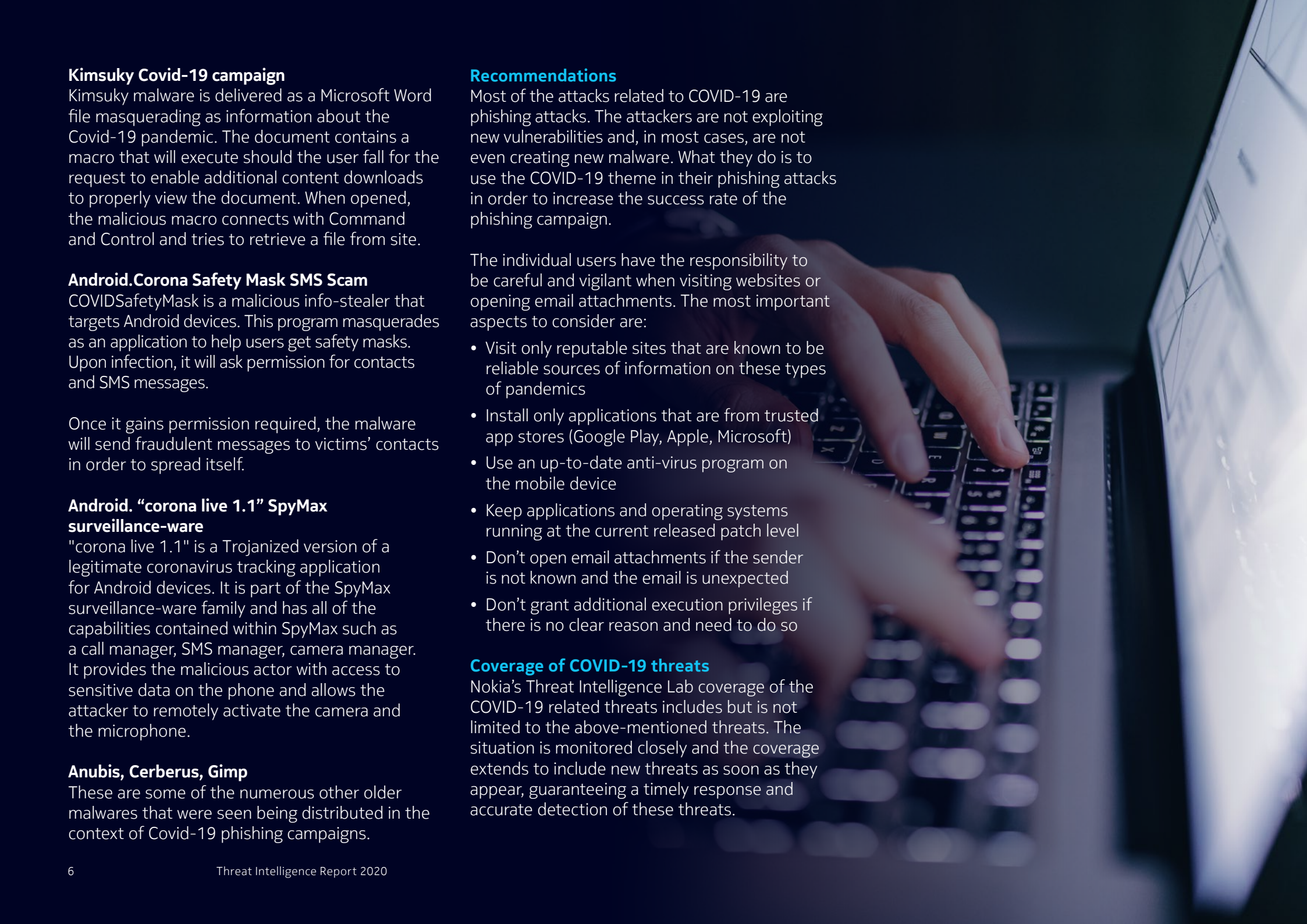
Most of the attacks related to COVID-19 are phishing attacks. The attackers are not exploiting new vulnerabilities and, in most cases, are not even creating new malware. What they do is to use the COVID-19 theme in their phishing attacks in order to increase the success rate of the phishing campaign.

The individual users have the responsibility to be careful and vigilant when visiting websites or opening email attachments. The most important aspects to consider are:

- Visit only reputable sites that are known to be reliable sources of information on these types of pandemics
- Install only applications that are from trusted app stores (Google Play, Apple, Microsoft)
- Use an up-to-date anti-virus program on the mobile device
- Keep applications and operating systems running at the current released patch level
- Don't open email attachments if the sender is not known and the email is unexpected
- Don't grant additional execution privileges if there is no clear reason and need to do so

Coverage of COVID-19 threats

Nokia's Threat Intelligence Lab coverage of the COVID-19 related threats includes but is not limited to the above-mentioned threats. The situation is monitored closely and the coverage extends to include new threats as soon as they appear, guaranteeing a timely response and accurate detection of these threats.



Malware in mobile networks

Mobile infection rate

Figure 2 shows the percentage of infected devices observed monthly since January 2019. This data has been averaged from mobile deployments in Europe, North America, Asia Pacific and the Middle East.

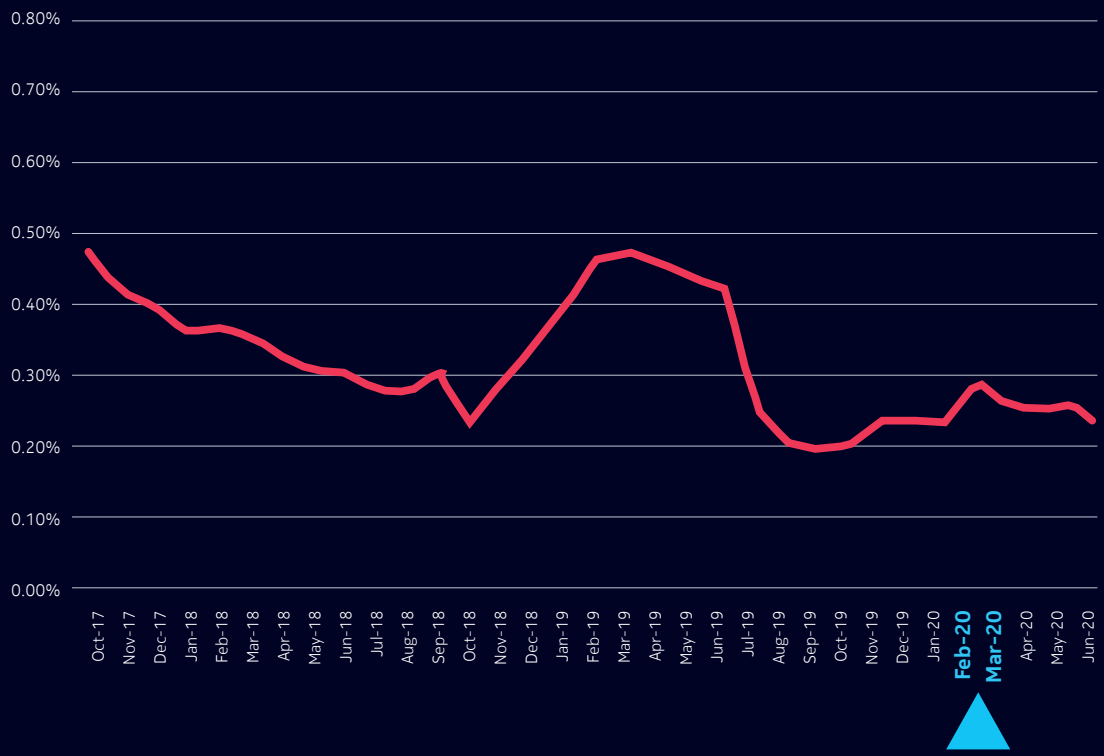
In 2020 the average percentage of devices infected each month was 0.23%. The peak was reached during the months of February and March, when the monthly mobile infection rate increased by almost 30% compared with the previous months. The reason for the increase is the significant escalation of cyber security incidents related to Covid-19. As presented in a previous section, the malicious actors were prompt in exploiting the opportunity offered by the spread of Covid-19.

As Nokia's NetGuard Endpoint Security solution is deployed in the networks of mobile internet service providers (ISPs) around the world, the increase in mobile infections was detected very early. By February, the increase was reflected in the monthly mobile infection rate.

As for the overall infection percentage, it is down from previous years. There are several explanations for this trend:

- Over the last few years, a significant improvement has been seen in the security of official mobile app stores. However, third-party app stores are still rife with Trojanized applications.
- The numbers come from networks protected by NetGuard Endpoint Security. This solution provides powerful mechanisms to help mobile ISPs detect and address cyber security issues in their mobile networks. NetGuard Endpoint Security also facilitates the notification of mobile subscribers of infections affecting their devices, so the subscribers can take actions by themselves. Therefore, as ISPs take action to actively reduce the rate of infection of their subscribers' devices, the mobile infection rate tends to be reduced over time.

Figure 2. Monthly mobile infection rates since January 2019



Infections by Device

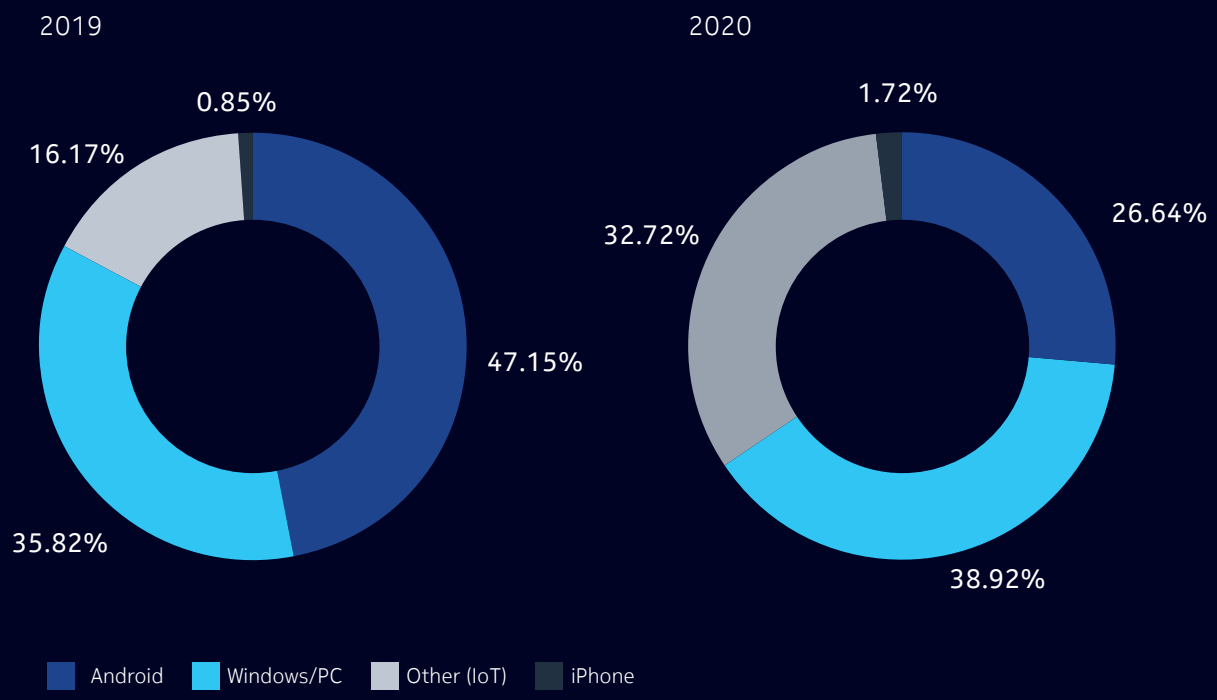
Figure 3 provides a breakdown of infections by device type in 2020. Among smartphones, Android devices are the most commonly targeted by malware. Android devices were responsible for 26.64% of all infections, Windows/PCs for 38.92%, IoT devices for 32.72% and only 1.72% for iPhones.

Comparing with 2019, the share occupied by infected Android devices has decreased, reflecting the shifting interest of the malicious actors toward IoT devices. Android-based devices still represent a major target in mobile networks.

In the smartphone sector, the main venue for distributing malware is represented by Trojanized applications. The user is tricked by phishing, advertising or other social engineering into downloading and installing the application. The security of official app stores, such as Google Play Store, has increased continuously. However, the fact that Android applications can be downloaded from just about anywhere still represents a huge problem, as users are free to download apps from third-party app stores, where many of the applications, while functional, are Trojanized. iPhones applications, on the other hand, are for the most part limited to one source, the Apple Store.

Windows/PCs are increasingly connected to the mobile network using USB dongles and mobile Wi-Fi devices or simply tethered through smartphones. Windows/PCs continue to be a target for malware infections, being responsible for almost 39% of the malware infections observed in 2020.

Figure 3. Infected device breakdown 2019 and 2020



Share of IoT infections has increased by 100%

IoT devices now make up 32.72% of the infected devices observed. Compared with 2019, the share occupied by IoT devices in the overall device breakdown has increased by 100%, from a previous share of 16.17%.

With the widespread proliferation of IoT devices, it is to be expected that the number of IoT infections will grow dramatically. As Figure 3 demonstrates, in 2020 this led to the increase of the share that IoT infections have in the overall device breakdown.

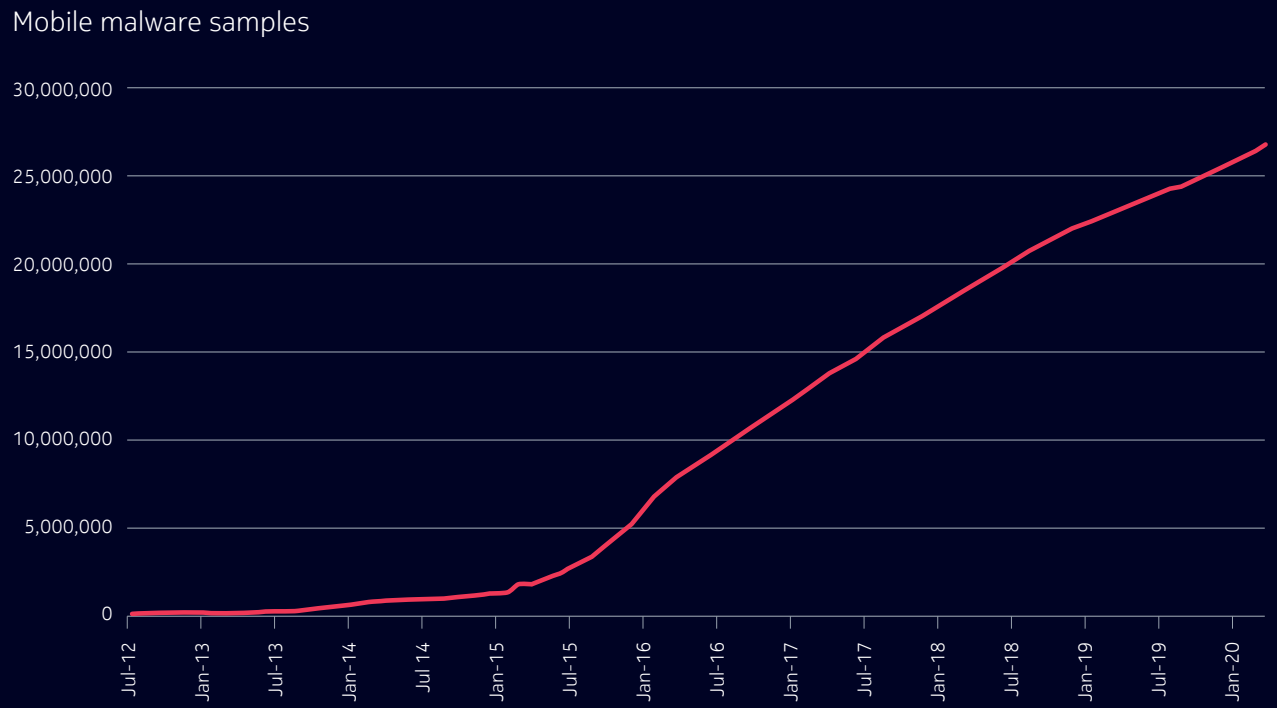
The rate of success in infecting IoT devices depends dramatically with the visibility of the devices to the internet. In networks where devices are routinely assigned public facing internet IP addresses, we find a high IoT infection rate. In networks where carrier grade NAT is used, the infection rate is considerably reduced, because the vulnerable devices are not visible to network scanning.

With the introduction of 5G well underway, it is expected that not only the number of IoT devices will increase dramatically, but also the share of IoT devices accessible directly from the internet will increase as well. A separate section of this report analyzes the security challenges in the 5G environment and highlights the important role that Threat Intelligence can play in addressing security issues in multiple systems of the 5G architecture.

Android malware samples continue to grow in 2020

Figure 4 shows the increase in the mobile malware samples that were collected and analyzed in the Threat Intelligence Lab. There are now close to 27 million Android malware samples, which represents a 17.4% year-over-year increase.

Figure 4. Mobile malware samples in Threat Intelligence Lab's database



Top Android malware

Figure 5. Top 20 Android malware detected in 2020

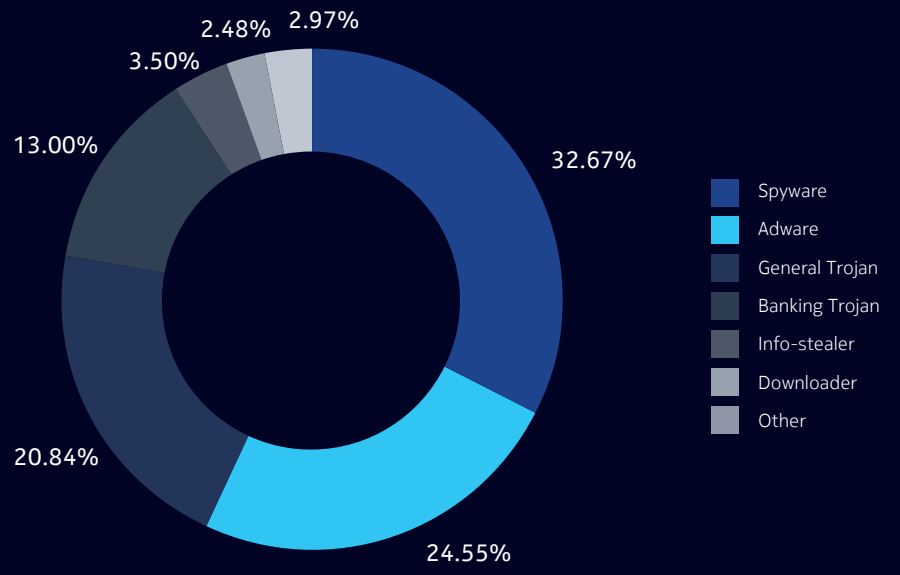
Name	Threat	%	Previous
Android.Adware.SimBad	Moderate	18.56	New
Android.BankingTrojan.GuStuff	High	9.37	New
Android.MobileSpyware.MobileTracker	High	8.55	New
Android.MobileSpyware.Xgen.YS	High	5.17	3.12
Android.Trojan.Hiddad.PL	High	5.07	New
Android.MobileSpyware.HoverWatch	High	5.06	New
Android.Spyware.mSpy	High	4.92	4.11
Android.Trojan.Click312.origin	High	4.32	New
Android.InfoStealer.Adups	High	3.09	3.03
Android.Adware.Updato	High	2.73	New
Android.MobileSpyware.iKeyMonitor	High	2.44	New
Android.Trojan.Hiddad.br	High	2.36	New
Android.MobileSpyware.Spyzie	High	2.22	New
Android.MobileSpyware.FlexiSpy	High	2.22	3.62
Android.Adware.Uapush.A	High	2.10	13.98
Android.Trojan.Rootnik.i	High	1.87	3.01
Android.BankingTrojan.Gugi.c	High	1.36	New
Android.Downloader.Agent.BLR	High	1.33	New
Android.Worm.ADB.miner	High	1.18	1.48
Android.Trojan.Gmobi.a	High	1.14	2.61

An interesting trend has been seen in the appearance and proliferation of new mobile spyware and info-stealers, with more than half of all Android malware falling into this category. These types of malware make up one-third of all infections detected in mobile networks — and when banking Trojans (a specialized form of info-stealer) are included, that percentage climbs to more than 50%.

Counting also the banking trojan, a specialized form of info stealer, the percentage surpasses 50%. This trend shows the shift of the interest of malicious actors toward stealing sensitive data and credentials, especially banking credentials. Adware remains a class very well represented, while infections with miners has decreased significantly (only one miner can be found among the Top 20 malwares, with a declining share).

Figure 6 illustrates the shares occupied by each type of Android malware as observed in 2020 in mobile networks around the world.

Figure 6. Android malware – breakdown by class type



Malware in fixed residential networks

Figure 7 shows residential infection rates since April 2017. These are reported on a monthly, per-residence basis, and then averaged across fixed network deployments of Nokia NetGuard Endpoint Security.

The average monthly residential infection rate for 2020 was 2.16%. Residential rates have been dropping consistently since 2015. The drop over the years can be attributed to:

- Cybercriminals are focusing their effort on IoT and mobile devices.
- Residential networks are better protected from the internet by the firewall features that are built into home routers.
- The operating systems and application used on modern laptop and desktop computers are more secure that the Windows/XP systems of the past.

One interesting aspect to note is that the monthly residential infection rate increased sharply in June 2020, almost doubling to 3.56%. This increase can be attributed to intensified phishing campaigns related to the Covid-19 pandemic.

This trend mirrors the trend observed in the case of mobile infections. As the residential infection rates reflect activity across fixed network deploy-ments of Nokia NetGuard Endpoint Security in North America, the increase of infection rates for fixed networks is delayed compared with the increase for mobile networks worldwide.

Figure 7. Monthly residential infection rate

Top 20 residential network infections

Figure 8. Top 20 home network infections

Name	Threat	%	Previous
Indep.Trojan.FakeApp.CQ	High	11.43	New
Android.Trojan.Hiddad.PL	High	8.57	New
Win32.BankingTrojan.Emotet	High	5.68	New
Android.Adware.SimBad	Moderate	4.40	New
Win32.HackerTool.TektonIt	High	3.26	3.75
MAC.Downloader.Shlayer	High	3.15	New
Win32.Hijacker.Altiress	High	2.35	New
Android.InfoStealer.Adups	High	2.16	1.3
Android.Trojan.Gmobi.a	High	2.11	New
Android.Trojan.HiddenApp	High	2.10	2.09
Win32.Adware.PullUpdate	Moderate	1.68	2.69
Win32.Adware.PullUpdate.A	Moderate	1.56	New
Android.Trojan.Hiddad.br	High	1.45	New
Win32.Worm.Fadok.A	High	1.45	New
Indep.SpamBot.GenericSpam	High	1.42	New
Win32.Downloader.Waledac.C	High	1.38	New
Win32.Hijacker.Diplugem	Moderate	1.24	1.79
Win32.Bot.ZeroAccess2	High	1.19	New
Win32.Downloader.InstallCore	High	1.16	2.25
Indep.Trojan.FakeApp.C	High	1.16	New

Figure 8 shows the top home network infections detected by Nokia NetGuard Endpoint Security solutions. The results are aggregated and the order is based on the number of infections detected over the period of this report.

Of the top 20 malware infections detected in fixed residential networks in 2020, the majority still focus on the traditional Windows/PC platform. Compared with the previous year, an increased number of Android malware infections has been detected in residential networks. This finding is consistent with the overall increase of the number of Android smartphones and the common practice of connecting smartphones to the internet via Wi-Fi when at home.

Top 20 high-level infections

Figure 9. Top 20 high-threat-level infections

Name	%	Previous	Previous
Indep.Trojan.FakeApp.CQ	13.80	New	New
Android.Trojan.Hiddad.PL	10.34	New	New
Win32.BankingTrojan.Emotet	6.86	New	New
Win32.HackerTool.TektonIt	3.93	5.63	New
MAC.Downloader.Shlayer	3.80	New	3.75
Win32.Hijacker.Altiress	2.84	1.6	New
Android.InfoStealer.Adups	2.61	1.96	New
Android.Trojan.Gmobi.a	2.54	1.22	1.3
Android.Trojan.HiddenApp	2.54	3.15	New
Win32.Worm.Fadok.A	1.75	1.24	2.09
Android.Trojan.Hiddad.br	1.75	New	2.69
Indep.SpamBot.GenericSpam	1.71	New	New
Win32.Downloader.Waledac.C	1.67	1.17	New
Win32.Bot.ZeroAccess2	1.43	New	New
Win32.Downloader.InstallCore	1.40	3.38	New
Indep.Trojan.FakeApp.C	1.40	New	New
Android.MobileSpyware.Xgen.YS	1.31	New	1.79
Indep.Trojan.DNSchanger	1.28	New	New
Indep.Bot.Mirai.variants	1.27	1.21	2.25
Android.Spyware.mSpy	1.27	New	New

Figure 9 shows the top 20 high-threat-level malware across both mobile and fixed networks. High threat level infections are associated with identity theft, financial loss and other cybercriminal activity.

The top 20 list contains a variety of bots, downloaders, banking Trojans and password stealers. It is remarkable that the most serious threats have maintained a stable presence, which shows the resilience of the APT groups and their ability to adapt and continue to be a serious threat over time.

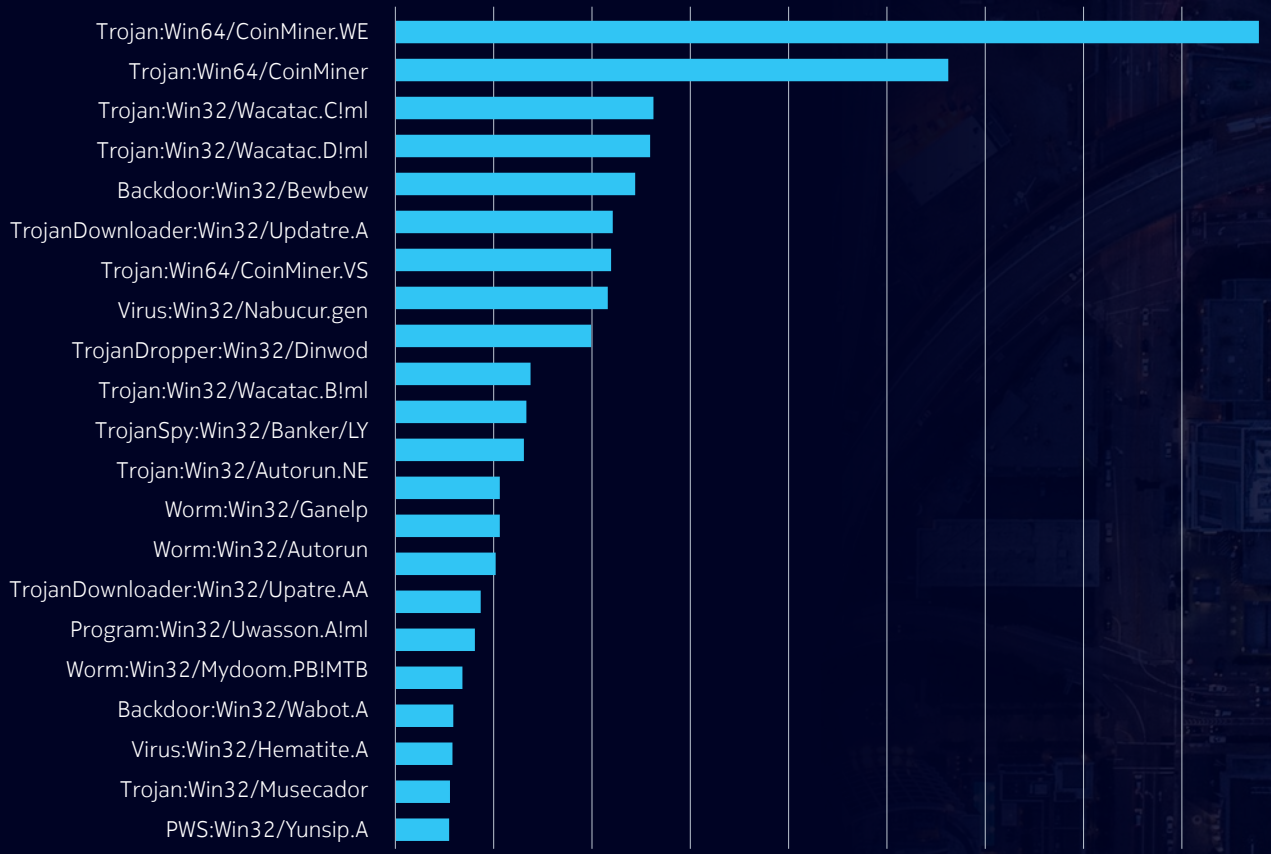
This year, Android malwares have increased their share in the top 20 high-threat infections list, from 3% to 7%.

Top 20 most prolific threats

A very good overview of the current cyber security trends can be obtained by analyzing the number of distinct samples captured from the internet at large.

Figure 10 shows the top 20 most prolific malware found on the internet. A large number of samples associated with a malware indicates that the malware was distributed through numerous Trojanized applications or is part of libraries widely used in application development. A prolific malware may also indicate that the malware author is making a serious attempt to evade detection by anti-virus products. Polymorphic malware constantly changes its identifiable features in order to make detection with anti-malware programs more difficult. Many of the common forms of malware can be polymorphic, including viruses, worms, bots, Trojans or keyloggers.

Figure 10. Top 20 most prolific malware



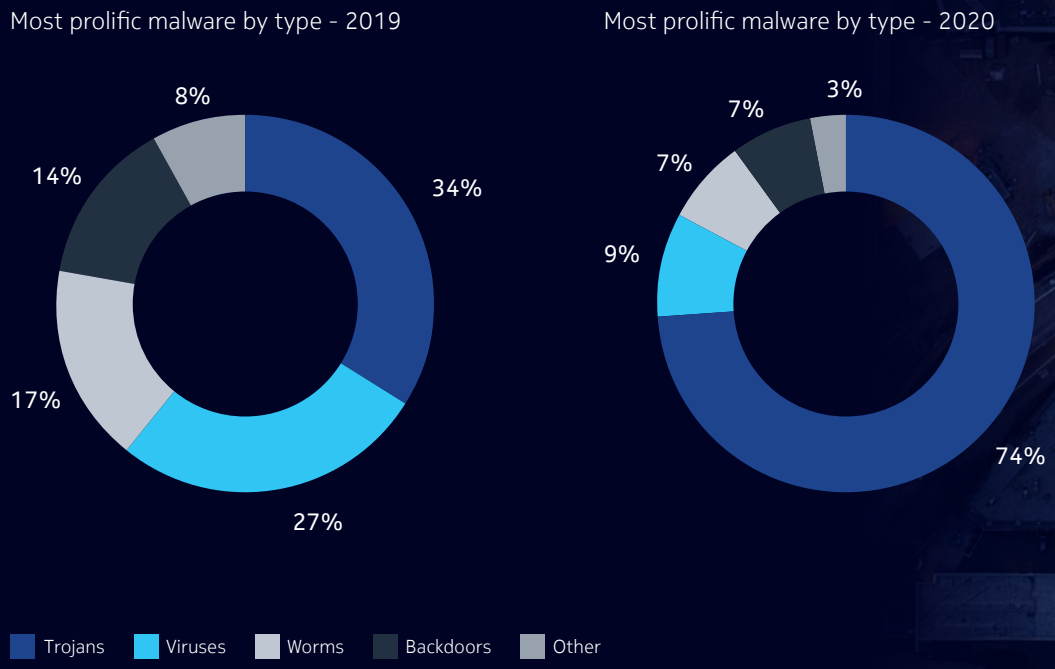
A prevalent type of cyber-crime is the cryptocurrency miner. It consumes intensively CPU and GPU resources of the system to secretly mine for cryptocurrency.

Another trend is the move toward malware dedicated to Win64 platform. The main reason for this trend is the ending of support for Windows 7.

Another type of malware that was prevalent in the last year is the info-stealer. These malwares aim to steal confidential data of users and share them with hackers. Also, they may allow remote access to the hackers to execute harmful tasks.

Figure 11 on the next page reveals a clear trend regarding the preferred method of malware distribution.

Figure 11. Most prolific malware by type in 2020



Threat intelligence takes a central role in 5G security

Architecture in transformation (technology shift)

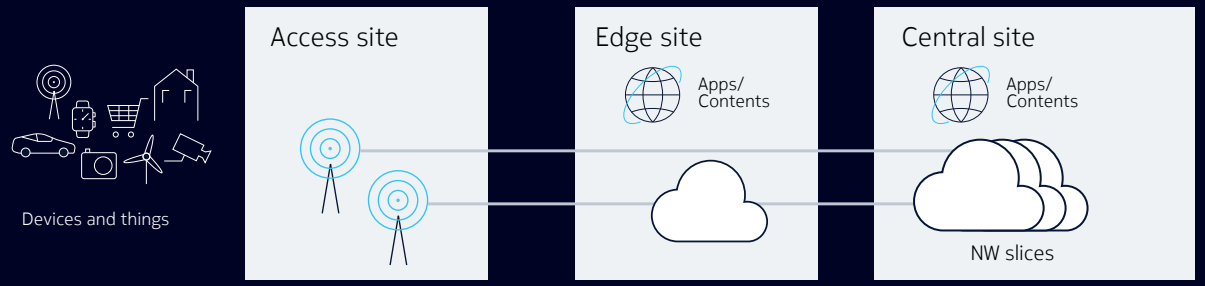
Consumers are looking forward to taking advantage of the benefits of 5G, including improved speed, lower latency, increased capacity and greater flexibility.

For communications service providers (CSPs), deploying 5G will be a challenge, mainly due to the sweeping changes in their current infrastructure. These changes are driven by the new technologies and paradigms that are specific to 5G.

The technologies listed below support fulfilling the main 5G requirements, including extremely fast control plane procedures, extremely low user plane latency and the highest degree of energy efficiency. At the same time, the introduction of these technologies brings about serious security challenges that will be discussed later.

Radio Access Network (RAN): The RAN is a collection of edge-located functions that connect a mobile device to the CSP's core network. Due to latency requirements and network load of 5G, the traditional ways of deploying RAN equipment are not well-suited for the new requirements. A new, cloud-based virtual RAN (vRAN) approach provides the necessary functionality for 5G; performance, flexibility and cost-efficiency that isn't available in fixed-function RAN equipment.

Figure 12. 5G overall architecture



Network Functions Virtualization (NFV): NFV decouples network functions, like firewall or encryption, from dedicated—and proprietary—hardware appliances, and instantiates them as software-based Virtual Network Functions (VNFs) on off-the-shelf servers that can be located on the customer premises, in the Communication Service Provider's network, or in the cloud.

Software-defined networking (SDN): The main concept is to decouple the infrastructure of wireless networks from expensive, closed hardware and shift it to an intelligent software layer running on commodity hardware.

Network slicing: One of the newest technologies enabled by 5G, it allows for different levels of security to be offered to users of different services. Each network slice is an isolated end-to-end network tailored to fulfill diverse requirements needed by each specific application.

Edge clouds: In a 5G mobile network architecture, most of the network functions run in cloud environments. What is specific to 5G is that these cloud environments are not restricted to central clouds but will comprise a number of highly distributed edge cloud deployments in order to facilitate mobile edge computing close to the mobile devices.

User scenarios evolving

On the consumer side, one of the defining features of 5G is the widening spectrum of stakeholders: CSPs may offer not only end-user communication services, but also provide complete virtual networks or "network slices" specialized for specific applications. These may be operated by various verticals, each one with specific requirements.

New user scenarios always introduce new security challenges, so it is important to review some of the scenarios that are going to benefit from 5G capabilities and are expected to experience widespread acceptance.

IoT: 5G networks are promising not only increased data rates but also low-latency data communication for time sensitive IoT applications. 5G will also enable connectivity of massive numbers of IoT devices. This will lead to more IoT applications where the devices not only act as sensors but increasingly interact with the real world.

M2M: Ubiquitous connectivity and guaranteed QoS in 5G will allow development of machine-to-machine networks. Connected devices communicate between themselves and with a centralized site that monitors and controls their operations, all automatically and without human intervention.

Real-time applications: From critical infrastructure to autonomous vehicles, 5G will allow a new type of applications that were not possible before, as the latency and resiliency were not high enough.

Security requirements and expectations from subscribers

It is clear that security will not only be fundamental to 5G success — it will be the major differentiator for service providers.

The success of 5G depends on the capability to ensure not only a high level of security and privacy for subscribers, but also to combat various forms of attacks against the integrity and availability of the services these networks provide. Privacy/encryption and authentication remain key. 5G networks must support a very high level of security and privacy for their users (not restricted to humans) and their traffic.

Availability becomes much more critical in the 5G era. This is due to the proliferation of serious applications (not only limited to data collection) in life-affecting verticals. In these cases, dependability of the network is paramount.

The subscribers of Communication Service Providers offering 5G services increasingly expect that their CSP provides a certain protection against cyber threats and are not left alone to deal with these threats. The customers will not only subscribe to communication services, but also cyber security services. Rapid and efficient responses to threats is expected from the CSP.

It is also essential to meet new regulatory requirements, as defined by 3GPP and the ETSI ISG NFV, the Open Networking Foundation (ONF) for software-defined networking, and the Internet Engineering Task Force (IETF).

Security threats – old and new (attacker shift)

The sweeping changes that are taking place in the 5G ecosystem open ample opportunities to malicious actors to take advantage of vulnerabilities of the new technologies.

For Communication Service Providers, it is a major challenge to provide a fully dependable, secure NFV environment. SDN bears the threat that control applications may wreak havoc on a large scale by erroneously or maliciously interacting with a central network controller. The network infrastructure of Communication Service Providers becomes more accessible to the attackers, so CSPs are increasingly targeted by sophisticated malicious actors.

Another window of opportunity for malicious actors is the appearance of new usage scenarios on the subscriber side. Each new usage scenario introduces new technologies, which leads to an increase of the attack surface.

At the same time, life-affecting usage scenarios will only increase the motivation of malicious actors, as there are more opportunities for inflicting damage and extracting ransom.

Security architecture for 5G

A robust security architecture for 5G needs to take into account the particularities of the 5G ecosystem, new usage scenarios and requirements/expectations regarding the level of security provided throughout.

It is therefore essential to:

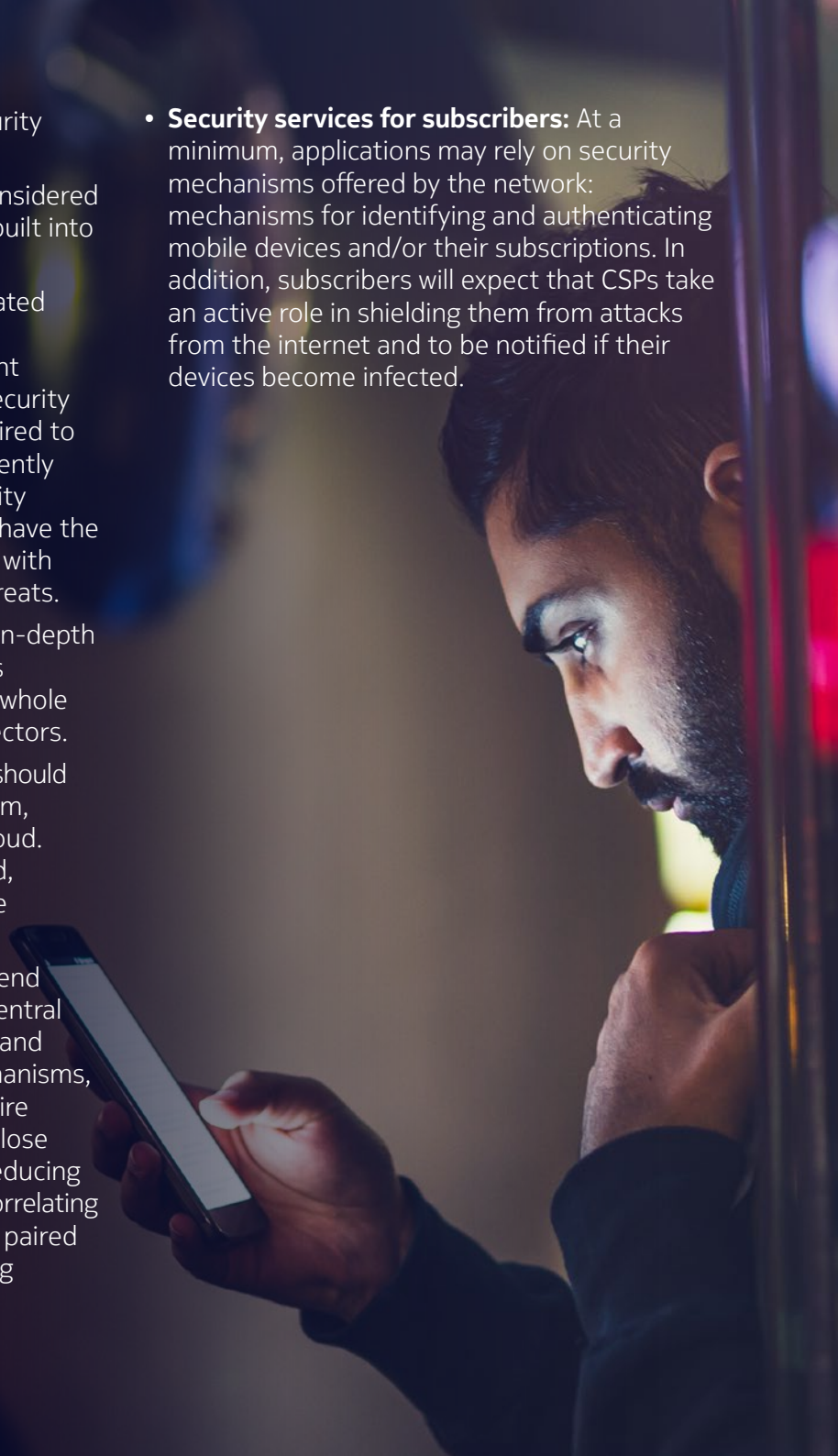
a) Consider security from the perspective of the subscribers. It is essential to support a variety of new use cases and identify trends. One concrete trend is the shift away from security controls at the device level (because of low resources). Another trend is the disappearance of perimeter security. Such trends lower the security posture of devices connected to the 5G network and places more responsibility on the CSP side.

b) Consider security from the perspective of the CSP. In the 5G era, CSPs will become themselves targets of attacks, with dire consequences for the availability of communication services offered to subscribers. It is also important to reconsider some current elements in the approach to security due to shifting networking paradigms, such as Network Functions Virtualization (NFV) and Software Defined Networking (SDN).

At the same time, CSPs must not only protect their infrastructure, but also play an increasingly significant role in providing security services to their subscribers.

The cornerstones of a successful 5G security architecture are:

- **Baked-in security:** Security must be considered as part of the overall architecture and built into the architecture right from the start.
- **Security automation:** Combine automated holistic security orchestration and management with automated, intelligent security controls. Automated holistic security orchestration and management is required to manage security efficiently and consistently throughout a network. Predictive security controls should act autonomously and have the capability to adapt themselves to cope with ever-changing and evolving security threats.
- **Redundancy:** A multi-layered defense-in-depth approach with intentional redundancies increases the security of a system as a whole and addresses many different attack vectors.
- **End-to-end security:** Security coverage should span all components of the 5G ecosystem, from device to CSP infrastructure to cloud. Any of the components can be attacked, compromising the security of the entire system.
- **Centralized security solution:** End-to-end security must be managed through a central point of control. This allows the set-up and maintenance of effective security mechanisms, as well as a secure operation of the entire network to help network operators disclose such activities at an early stage, thus reducing greater harm. This can be achieved by correlating data from systems across the network, paired with automated workflows for triggering countermeasures.
- **Security services for subscribers:** At a minimum, applications may rely on security mechanisms offered by the network: mechanisms for identifying and authenticating mobile devices and/or their subscriptions. In addition, subscribers will expect that CSPs take an active role in shielding them from attacks from the internet and to be notified if their devices become infected.



Threat Intelligence takes the center stage

Threat intelligence has always played an essential role in the success of any security solution. Both the host-based and network-based security appliances cannot perform without up-to-date threat intelligence.

In the 5G context, due to the complex 5G network architecture, new use cases and new security architectures, additional requirements are placed on threat intelligence.

- **Increased accuracy:** As mentioned before, 5G security relies increasingly on automation. The goal of automation is to take quick action upon detection of incidents, rather than just alerting a human operator who then evaluates the incident and takes action if the incident is deemed real and of a high enough severity. In this context, there is no room for false positives, as actions taken based on false positives can be very detrimental to the functioning and security of the entire system.
- **Increased coverage:** Traditionally, security systems are targeting the protection of end user devices. However, in the case of 5G, the distributed infrastructure of Communication Service Providers may also be targeted by malicious actors, so protection needs to be extended to cover those components as well. From a threat intelligence perspective, this amounts to a substantial increase in coverage necessary to protect the network assets.
- **Correlation between attacks and post-infection activity:** Correlating observed attacks with security incidents inside the system can bring a lot of value by providing various clues leading up to a security incident. In a complex distributed system like 5G, this correlation becomes even more valuable for the automatic evaluation of security incidents and the initiation of preventative countermeasures.
- **Good priority classification:** It is always important to know if immediate action is required or alerting operators is sufficient. In the case of automatic security systems, this knowledge becomes even more important because it is not desirable to have a system that is over-reactive and performs potentially significant countermeasures if it is not necessary.
- **Solid security requirements for what could be impacted must be defined:** As automated workflows are increasingly used for triggering countermeasures, it is essential to be able to predict the malware actions upon infection. This allows for taking preventive actions before the malware attempts to perform its malicious actions.
- **Coverage of all phases of attacks:** Threat intelligence need to cover all the phases of a cyber-attack, from discovery and initial attack to post-infection activities, lateral movement, data exfiltration and host exploitation (DDoS attacks, etc). Only by having accurate threat intelligence is it possible to detect malicious activity and automatically take preventive/corrective actions during all phases of the attack.

In the 5G system, there are multiple areas where threat intelligence is used by various components of the security architecture.

Network-based security solutions

5G offers security features focused on the interface between mobile devices and the network (e.g., IPSec tunnels to protect the data between the base stations and the core network, identification and authentication), but doesn't do anything to protect the devices against attacks.

Subscriber's devices, often without the owner's knowledge, can be corrupted by malware and attack the network. At its most dangerous, many corrupted devices may form a mobile botnet that carries out large-scale attacks against the network. Future networks will suffer due to a continuous increase of IoT botnets like Mirai or toolkits for mobile devices like DroidJack, which has recently been used to attack web services and network infrastructure.

Host-based security solutions are not a good solution for protecting the devices connected to the 5G network, as most of them have limited resources.

As a result, network-based detection of suspicious device behaviour on Internet Protocol (IP), as well as application layer protocols, becomes imperative as it protects not only subscribers and the data on their devices, but also the networks themselves. Network-based detection scales well with the exponential increase in the number of devices connected to 5G networks, and provides very good detection of attacks and post-infection activity (e.g., propagation, command and control communication and other malicious actions).

With the role of network-based security solutions increasing in importance in 5G networks, the quality of threat intelligence that powers them needs to increase in terms of coverage, accuracy, etc.

Security Orchestration

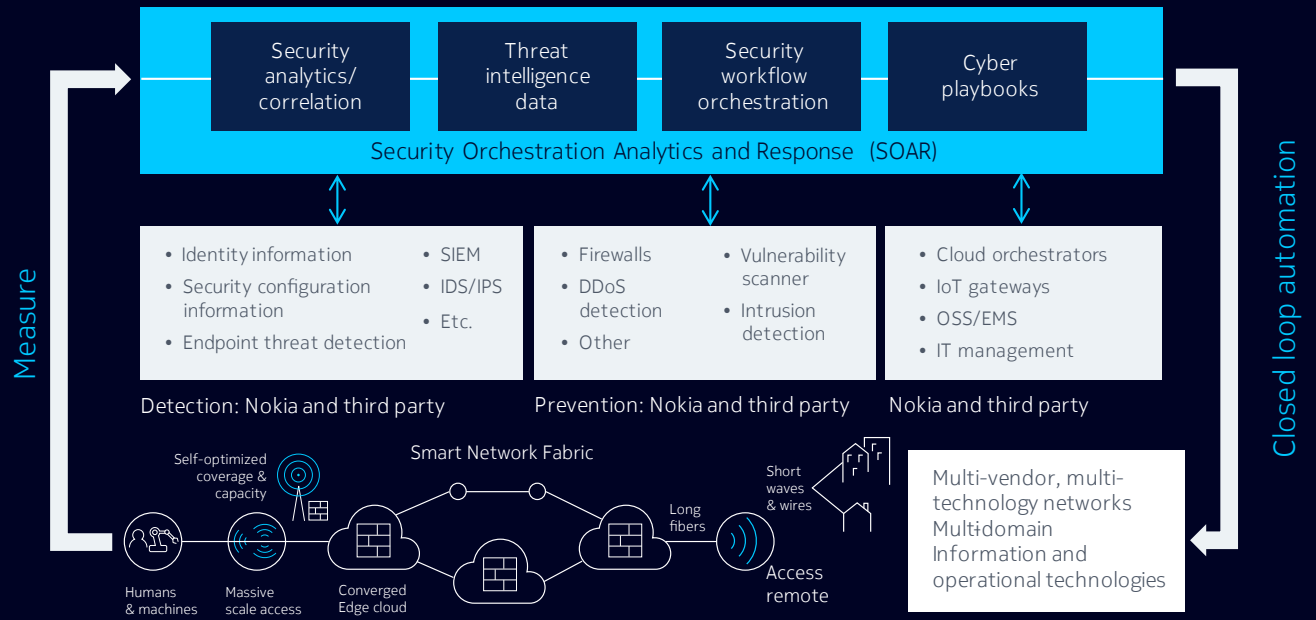
Security Orchestration, Automation and Response (SOAR) technology has emerged as the primary choice for ensuring security of 5G networks. It allows for the streamlining of security operations in three key areas: threat and vulnerability management, incident response, and security operations automation.

Threat intelligence plays a key role in elevating the performance of the SOAR solution. As it relates to security automation (the automatic handling of security operations-related tasks), threat intelligence plays a central role in the analysis of vulnerability and threat data received from multiple sources.

There are several use cases where the SOAR platform benefits from threat intelligence:

- **Endpoint diagnostics**
  Threat intelligence helps to efficiently manage the overwhelming number of alerts from logs and various data feeds, assess the risk of new indicators and respond to endpoint threats proactively.
- **Vulnerability management**
  SOAR platform needs to rapidly identify emerging threats before they actually hit targets in the 5G networks. Threat intelligence helps identifying the security measures that are necessary to protect the system before attacks happen.

Figure 13. Areas where Threat Intelligence (TI) plays a central role



CSP and cloud infrastructure

Threat intelligence plays a critical role in protecting the infrastructure of Communication Service Providers. In the 5G world, most of the network functions are expected to run in Network Functions Virtualization (NFV) environments or the cloud. Attacks on NFVs can have a devastating impact on the capability of telcos to offer services and, as a result, can affect the availability of communication services to subscribers.

There are multiple NFV cyber security challenges that need to be overcome:

- **Security pitfalls of OpenStack:** Protect OpenStack controller and OpenStack compute nodes where, in telecom NFV networks, the compute nodes are outside of the core.
- **Both the data plane and the control plane are implemented in software:** This increases the attack surface and increases the risks for an successful attack.
- **The control plane of each function is open for remote operation:** With NFV, an entire host can be programmed by an external controller, which provides the opportunity for those devices to be taken over by a malicious actor.
- **Malware may propagate easily across VMs and hosts:** The challenge with NFV is that the entire network is made up of hosting machines that run a virtualization environment. Being outside the security perimeter, malware software can propagate itself throughout the network.

Conclusion

The outbreak of the COVID-19 pandemic has ensured that 2020 is a remarkable year from the perspective of the security of mobile and fixed networks. The volume and type of attacks have seen profound changes. Nokia's NetGuard Endpoint Security, which is deployed in the networks of mobile and fixed ISPs around the world, was best prepared to capture the new trends and to help the Internet providers to improve the security posture of their networks and of their subscribers.

In 2020, the average monthly infection rate in mobile networks was 0.23%. In fixed broadband networks, the monthly infection rate per residence was 2.16%. While the average infection rates are down from previous years, there are considerable variations due to specific circumstances.

About the Nokia Threat Intelligence Lab

The Nokia Threat Intelligence Lab focuses on the behavior of malware network communications to develop detection rules that identify malware infections based on command-and-control communication and other network behavior. This approach enables the detection of malware in the service provider's network and the detection rules developed form the foundation of Nokia's network-based malware detection product suite.

To accurately detect that a user is infected, our detection rule set looks for network behavior that provides unequivocal evidence of infection coming from the user's device. This behavior includes:

- Malware command-and-control (C&C) communications
- Backdoor connections
- Attempts to infect others (for example, exploits)
- Excessive email
- Denial of Service (DoS) and hacking activity

Four main activities support our signature development and verification process:

1. Monitor information sources from major security vendors and maintain a database of currently active threats
2. Collect malware samples (>200,000/day), classify and correlate them against the threat database
3. Execute samples matching the top threats in a sandbox environment and compare against our current signature set
4. Conduct a detailed analysis of the malware's behavior and build a new signature, if a sample fails to trigger a signature

For more information please visit:

Nokia Threat Intelligence Center

End-to-end security portfolio page

Endpoint security solutions page

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Document code: CID210088 (October)

About Nokia

We create the technology to connect the world. Only Nokia offers a comprehensive portfolio of network equipment, software, services and licensing opportunities across the globe. With our commitment to innovation, driven by the award-winning Nokia Bell Labs, we are a leader in the development and deployment of 5G networks.

Our communications service provider customers support more than 6.4 billion subscriptions with our radio networks, and our enterprise customers have deployed over 1,300 industrial networks worldwide. Adhering to the highest ethical standards, we transform how people live, work and communicate. For our latest updates, please visit us online www.nokia.com and follow us on Twitter @nokia.