spyware

Staying safe from Pegasus, Chrysaor and other APT mobile malware

How to protect your iPhone or Android smartphone from Pegasus and similar mobile APTs.

Costin Raiu

February 3, 2022

Possibly the biggest story of 2021 — an investigation by the Guardian and 16 other media organizations, published in July — suggested that over 30,000

alleged that the malware was deployed widely through a variety of exploits, including several iOS zero-click zero-days.

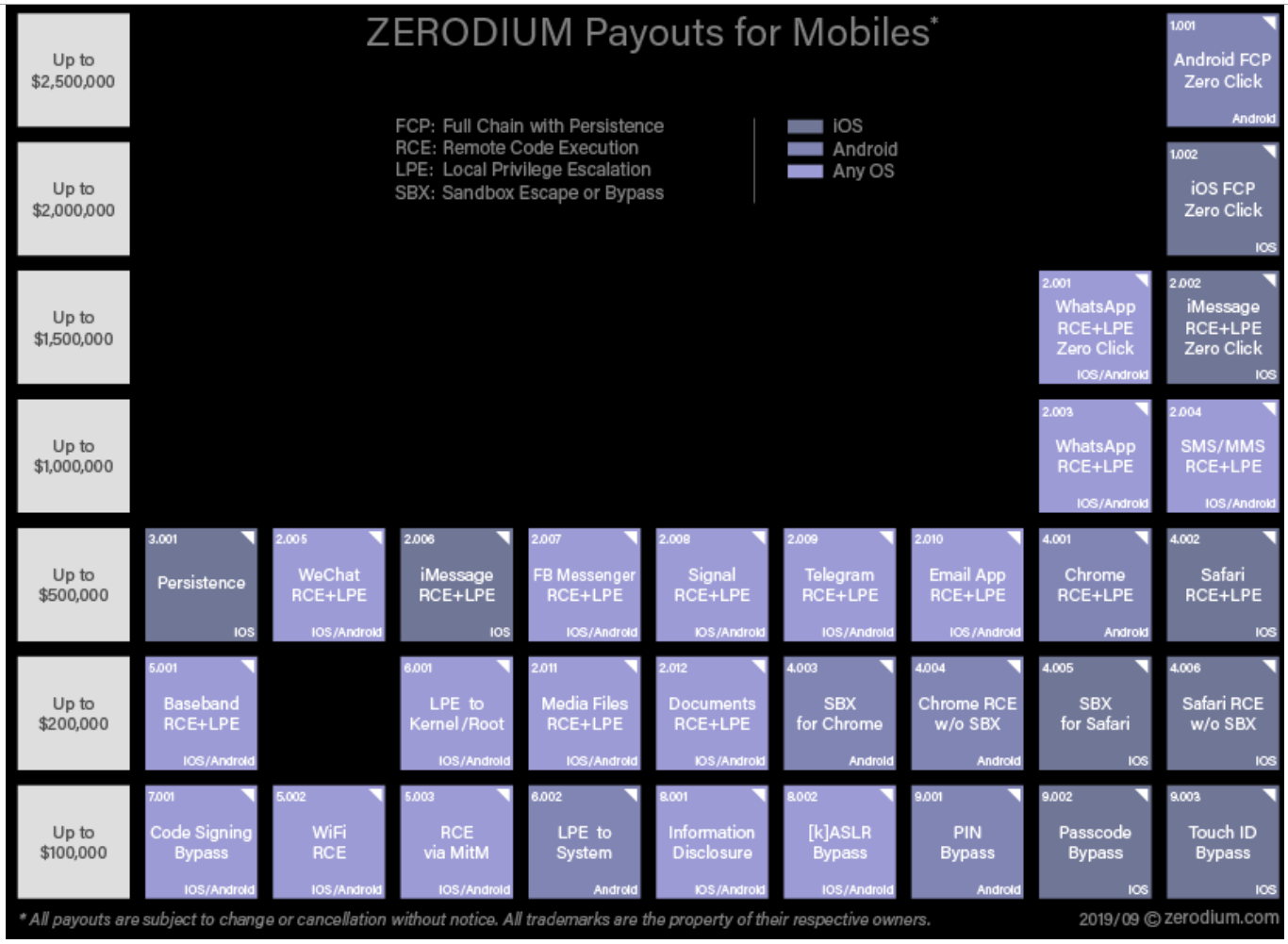
Based on forensic analysis of numerous mobile devices, Amnesty International's Security Lab found that the software was repeatedly used in an abusive manner for surveillance. The list of targeted individuals includes 14 world leaders and many other activists, human rights advocates, dissidents and opposition figures.

Later in July, representatives from the Israeli government visited the offices of NSO as part of an investigation into the claims. In October, India's Supreme Court commissioned a technical committee to investigate the use of Pegasus to spy on its citizens. Apple announced, in November, that it was taking legal action against NSO Group for developing software that targets its users with "malicious malware and spyware." Last but not least, in December, Reuters published that US State Department phones were hacked with the NSO Pegasus malware, as alerted by Apple.

Over the past few months I have received a lot of questions from concerned users worldwide on how to protect their mobile devices from Pegasus and other similar tools and malware. We are trying to address this in the current article, with the observation that no list of defence techniques can ever be exhaustive. Additionally, as attackers change their modus operandi, protection techniques should also be adapted.

How to stay safe from Pegasus and other advanced mobile spyware

First of all, we should start by saying that **Pegasus is a toolkit sold to nation states at relatively high prices**. The cost of a full deployment may easily reach millions of USD. Similarly, other APT mobile malware may be deployed through zero-click 0-day exploits. These are extremely expensive — as an example, Zerodium, an exploit brokerage firm pays up to $2.5 million for an Android zero-click infection chain with persistence:



From the start, this draws an important conclusion — nation state sponsored cyberespionage is a vastly resourceful endeavor. When a threat actor can afford to spend millions, potentially tens of millions or even hundreds of millions of USD on their offensive programs, it is very unlikely that a target will be able to avoid getting infected. To put this in simpler words, if you are targeted by such an actor, it's not a question of "whether you can get infected," it's actually **just a matter of time and resources before you get infected**.

Now, for the good news — exploit development and offensive cyberwarfare are often more of an art rather than an exact science. Exploits need to be tuned for specific OS versions and hardware and can be easily thwarted by new OS releases, new mitigation techniques or even small things such as random events.

With that in mind, infection and targeting is also a question of cost and making things more difficult for the attackers. Although we may not always be able to prevent the successful exploitation and infection of the mobile device, we can try

How to protect from advanced spyware on iOS

Reboot daily. According to research from Amnesty International and Citizen Lab, the Pegasus infection chain often relies on zero-click 0-days with no persistence, so regular reboot helps clean the device. If the device is rebooted daily, the attackers will have to re-infect it over and over again. In time, this increases the chances of detection; a crash might happen or artifacts could be logged that give away the stealthy nature of the infection. Actually, this is not just theory, it's practice — we analyzed one case in which a mobile device was targeted through a zero-click exploit (likely FORCEDENTRY). The device owner rebooted their device regularly and did so in the next 24 hours following the attack. The attackers tried to target them a few more times but eventually gave up after getting kicked a few times through reboots.

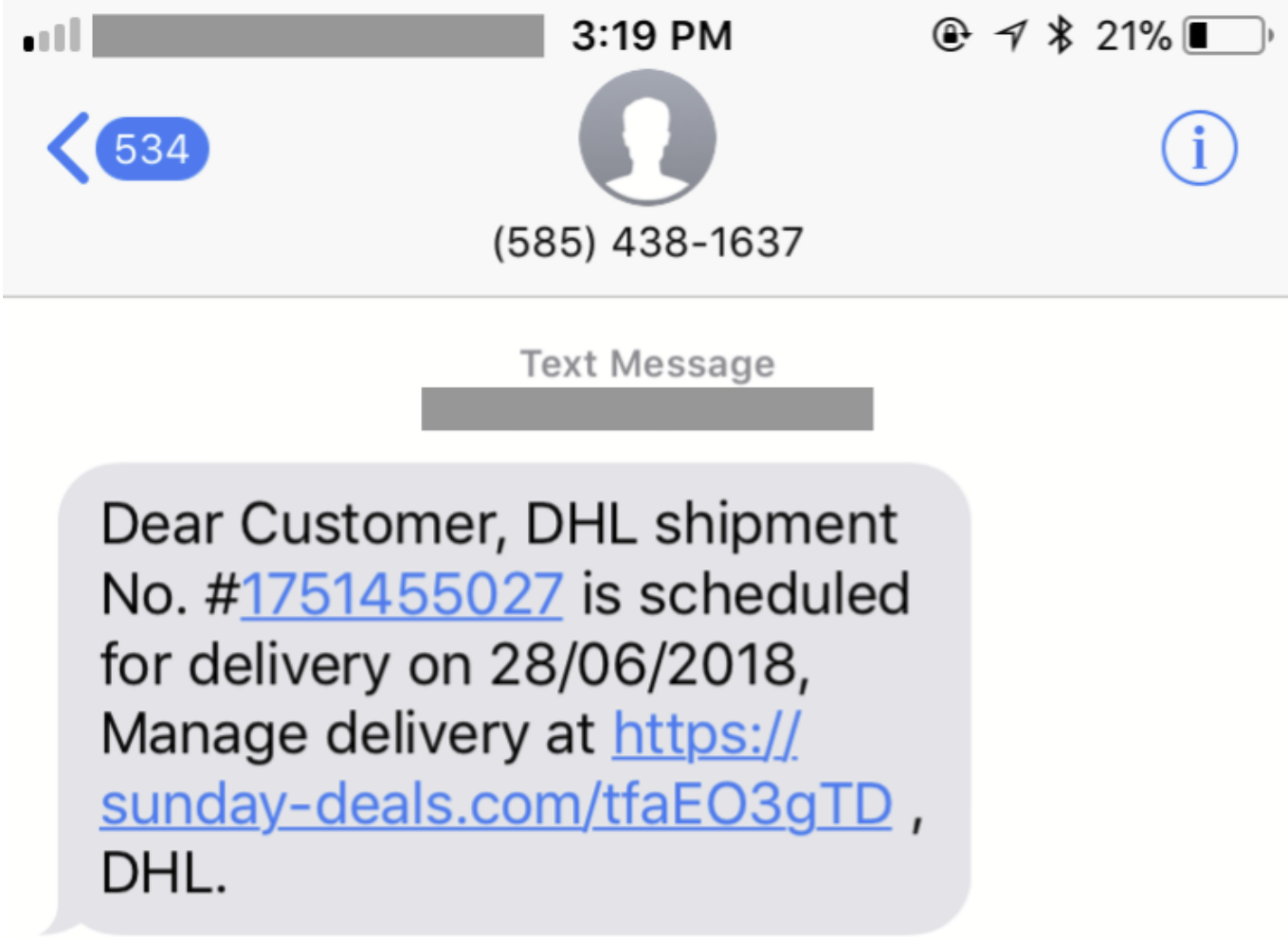
NoReboot: A fake restart to gain a foothold in the system

Disable iMessage. iMessage is built into iOS and is enabled by default, making it an attractive exploitation vector. Because it's enabled by default, it is a top delivery mechanism for zero-click chains and for many years, iMessage exploits were in high demand, with top payouts at exploit brokerage companies. "During the last few months, we have observed an increase in the number of iOS exploits, mostly Safari and iMessage chains, being developed and sold by researchers from all around the world. **The zero-day market is so flooded by iOS exploits that we've recently started refusing some (of) them**," Zerodium's founder Chaouki Bekrar wrote back in 2019 to WIRED. We realize life without iMessage may be very difficult for some (more on that later), but if Pegasus and other high-end APT mobile malware is in your threat model, this is a tradeoff worth taking.

Disable Facetime. Same advice as above.

Keep the mobile device up to date; install the latest iOS patches as soon as they are out. Not everyone can afford zero-click 0-day's, actually many of the iOS exploit kits we are seeing are targeting already patched vulnerabilities.

Don't ever click on links received in messages. This is simple advice yet effective. Not all Pegasus customers can afford to buy zero-click 0-day chains at a cost of millions so they rely on 1-click exploits. These arrive in the form of a message, sometimes by SMS, but can also be via other messengers or even e-mail. If you receive an interesting SMS (or by any other messenger) with a link, open it on a desktop computer, preferably using TOR Browser, or better yet using a secure non-persistent OS such as Tails.



SMS with a malicious link used to target a political activist. Source: Citizen Lab

Browse the Internet with an alternate browser such as Firefox Focus instead of Safari or Chrome. Despite the fact that all browsers on iOS pretty much use the same engine, Webkit, some exploits do not work well (see LightRighter / TwoSailJunk APT case) on some alternate browsers:

```
detect_os()

return {
        mobile: (typeof window.orientation !== "undefined") || (navigator.userAgent.indexOf('IEMobile') !== -1),
        webkit: parseFloat(/AppleWebKit\/([\d.]+)/.exec(navigator.userAgent)[1]) || 0,
        safari: window.navigator.userAgent.indexOf('Safari') > -1,
        version: function()
        {
                var match = (navigator.appVersion).match(/OS (\d+)_(\d+)_?(\d+)?/);
        if(match) {
                var version = [
                    parseInt(match[1], 10),
                    parseInt(match[2], 10),
                    parseInt(match[3] || 0, 10)
                        ];
                        return parseFloat(version[0]+'.'+version[1]+version[2]);
            } else {
                return "unknown";
```

LightRiver exploit kit check for “Safari” in the user agent string

User agent strings on iOS from Safari, Chrome and Firefox Focus browsers:

Safari: Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Mobile/15E148 Safari/604.1

Chrome: Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/96.0.4664.53 Mobile/15E148 Safari/604.1

Firefox Focus: Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) FxiOS/39 Mobile/15E148 Version/15.0

Always use a VPN that masks your traffic. Some exploits are delivered through GSM operator MitM attacks, when browsing HTTP sites or by DNS hijack. Using a VPN to mask the traffic makes it difficult for your GSM operator to target you directly over the Internet. It also complicates the targeting process if the attackers have control over your data stream, such as while in roaming. Please note that not all VPNs are the same and not any VPN is fine to use. Without favoring any specific VPN provider, here’s a few things to consider when you shop for a VPN subscription with anonymity being a top priority:

Purchase means just that — **no “free” VPNs.**

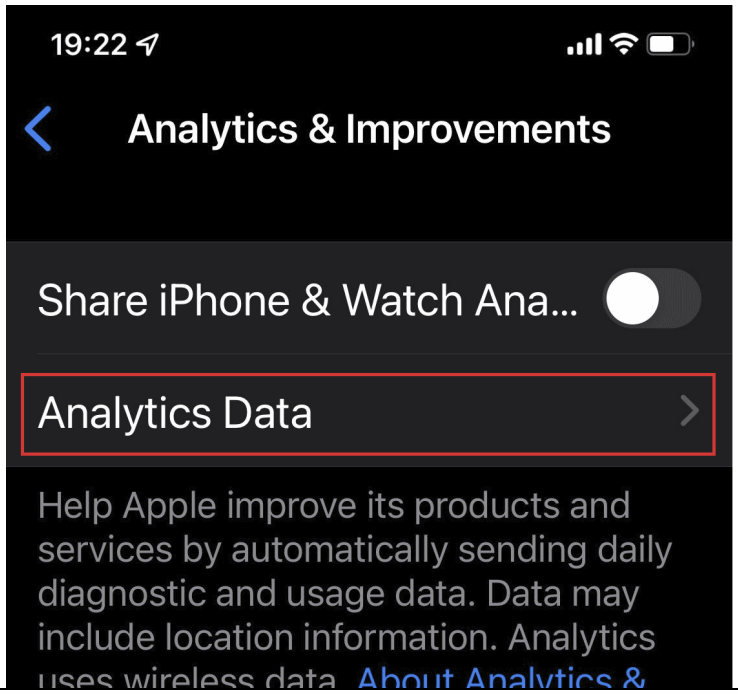
Try to avoid VPN apps — instead, use open-source tools such as OpenVPN, WireGuard and VPN profiles.

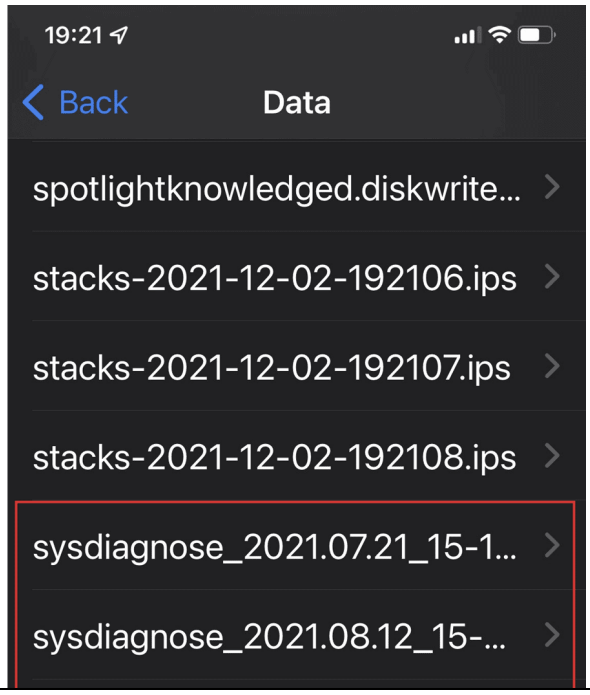
Avoid new VPN services and look for established services that have been around for some time.

Install a security application that checks and warns if the device is jailbroken. Frustrated from getting kicked over and over, the attackers will eventually deploy a persistence mechanism and jailbreak your device in the process. This is where the chance of catching them increases tenfold and we can take advantage of the fact that the device is jailbroken.

Make iTunes backups once per month. this allows diagnosing and finding infections later, through the use of the wonderful MVT package from Amnesty International (more on that later).

Trigger sysdiags often and save them to external backups. Forensics artifacts can help you determine at a later time if you have been targeted. Triggering a sysdiag depends on the phone model — for instance, on some iPhone's, this is done by pressing *Volume Up + Volume Down + Power* at the same time. You may need to play with this a couple of times, until the phone buzzes. Once the sysdiag is created, it will appear in diagnostics:





How to protect from advanced spyware on Android

A similar list for Android users (for details and reasoning check the list for iOS above):

Reboot daily. Persistence on the latest Android versions is difficult, many APTs and exploit sellers avoid persistence whatsoever!

Keep phone up to date; install latest patches.

Don't ever click on links received in text messages.

Browse the internet with an alternate browser such as Firefox Focus instead of the default Chrome.

Always use a VPN that masks your traffic. Some exploits are delivered through GSM operator MitM attacks, when browsing HTTP sites or by DNS hijack.

Install a security suite that scans for malware and checks and warns if the device is rooted.

At a more sophisticated level — both for iOS and Android — always check your network traffic using live IoCs. A good setup might include a Wireguard always-on VPN to a server under your control, that uses pihole to filter out bad stuff and logs all the traffic for further inspection.

How to get by without iMessage

I was talking to my friend Ryan Naraine recently, and he said — *"iMessage and FaceTime — these are **the** reasons why people use iPhones!"* and for sure, he's right. I've myself been an iPhone user since 2008 and think iMessage and FaceTime were two of the greatest things Apple added to this ecosystem. When I realized that these are also some of the most exploited features that let nation states spy on your phone, I tried to escape the iMessage Hotel California. The hardest thing? Getting the family to stop using it too. Surprising as it may sound, this was one of the most difficult things in this whole security saga.

At first, I tried to switch everyone to Telegram. This didn't go too well. Then, Signal got better and better, implemented Video calls and group calling. In time, more and more friends started moving to Signal. And this worked well with my family too. I'm not saying you should do the same. Perhaps you can keep iMessage enabled and live happily and malware free — truth be told, Apple greatly improved the security sandbox around iMessage with BlastDoor in iOS 14. Nevertheless, the FORCEDENTRY exploit used by NSO to deliver Pegasus bypassed BlastDoor and of course, no security feature is ever 100% hack-proof.

So, what is the best of both worlds, you may ask? Some people, including myself,

phone number. If someone decides to target me this way, there's a good chance they will end up in the honeypot phone.

How to detect Pegasus and other advanced mobile malware

Detecting infection traces from Pegasus and other advanced mobile malware is very tricky, and complicated by the security features of modern operating systems such as iOS and Android. Based on our observations, this is further complicated by the deployment of non-persistent malware, which leaves almost no traces after reboot. Since many forensics frameworks require a device jailbreak, which in turn requires a reboot, this results in the malware being removed from memory during the reboot.

Currently, several methods can be used for detection of Pegasus and other mobile malware. MVT (Mobile Verification Toolkit) from Amnesty International is free, open source and allows technologists and investigators to inspect mobile phones for signs of infection. MVT is further boosted by a list of IoCs (indicators of compromise) collected from high profile cases and made available by Amnesty International.

What to do if you got infected with Pegasus

So you followed all these recommendations carefully and still got infected. Sadly, this is the reality we live in nowadays. I feel for you, really. You may not be a bad guy at all — on the contrary, I'm sure you're one of the good guys. Perhaps you spoke against powerful people, or participated in some protests against a questionable decision from certain political figures, or simply used encryption software or been in the wrong place at the wrong time. Look on the bright side — you *know* you've been infected, because artifacts and knowledge allowed you to determine that. Think of the following things:

Who targeted you and why? Try to figure out what it was that brought you into the attention of the big guys. Is this something that you can avoid in the future through more stealthy behavior?

Can you speak about it? The thing that eventually brought down many surveillance companies was bad publicity. Reporters and journalists writing about abuses and exposing the lies, wrongdoing and all the evil. If you've been targeted try to find a journalist and tell them your story.

Change your device — if you were on iOS, try moving to Android for a while. If you were on Android, move to iOS. This might confuse attackers for some time; for instance, some threat actors are known to have purchased exploitation systems that only work on a certain brand of phone and OS.

Get a secondary device, preferably running GrapheneOS, for secure comms. Use a prepaid card in it, or, only connect by Wi-Fi and TOR while in airplane mode.

Avoid messengers where you need to provide your contacts with your phone number. Once an attacker has your phone number they can easily target you across many different messengers via this — iMessage, WhatsApp, Signal, Telegram, they are all tied to your phone number. An interesting new choice here is Session, which automatically routes your messages through an Onion-style network and doesn't rely on phone numbers.

100% proof; think of it like a stream that flows and you need to adjust your sailing depending on the speed, currents and obstacles.

At the end of this, I'd like to leave you with a thought. If you get targeted by nation states, that means **you are important**. Remember: it's nice to be important, but it's more important to be nice. Alone, we are weak, together, we are strong. The world may be broken, but I believe we are living at a time when we can still change things. According to a report from the nonprofit group Committee to

how the world will look like for us in 10 years, for our children and our children's children.

You, the people have the power — the power to create machines. The power to create happiness! You, the people, have the power to make this life free and beautiful, to make this life a wonderful adventure.

Then — in the name of democracy — let us use that power — let us all unite. Let us fight for a new world — a decent world that will give men a chance to work — that will give youth a future and old age a security. By the promise of these things, brutes have risen to power. But they lie! They do not fulfil that promise. They never will!

Dictators free themselves but they enslave the people! Now let us fight to fulfil that promise! Let us fight to free the world — to do away with national barriers — to do away with greed, with hate and intolerance. Let us fight for a world of reason, a world where science and progress will lead to all men's happiness. Soldiers! in the name of democracy, let us all unite!

Final speech from The Great Dictator

This post originally ran as a series of op-eds in Dark Reading (part 1, part 2).

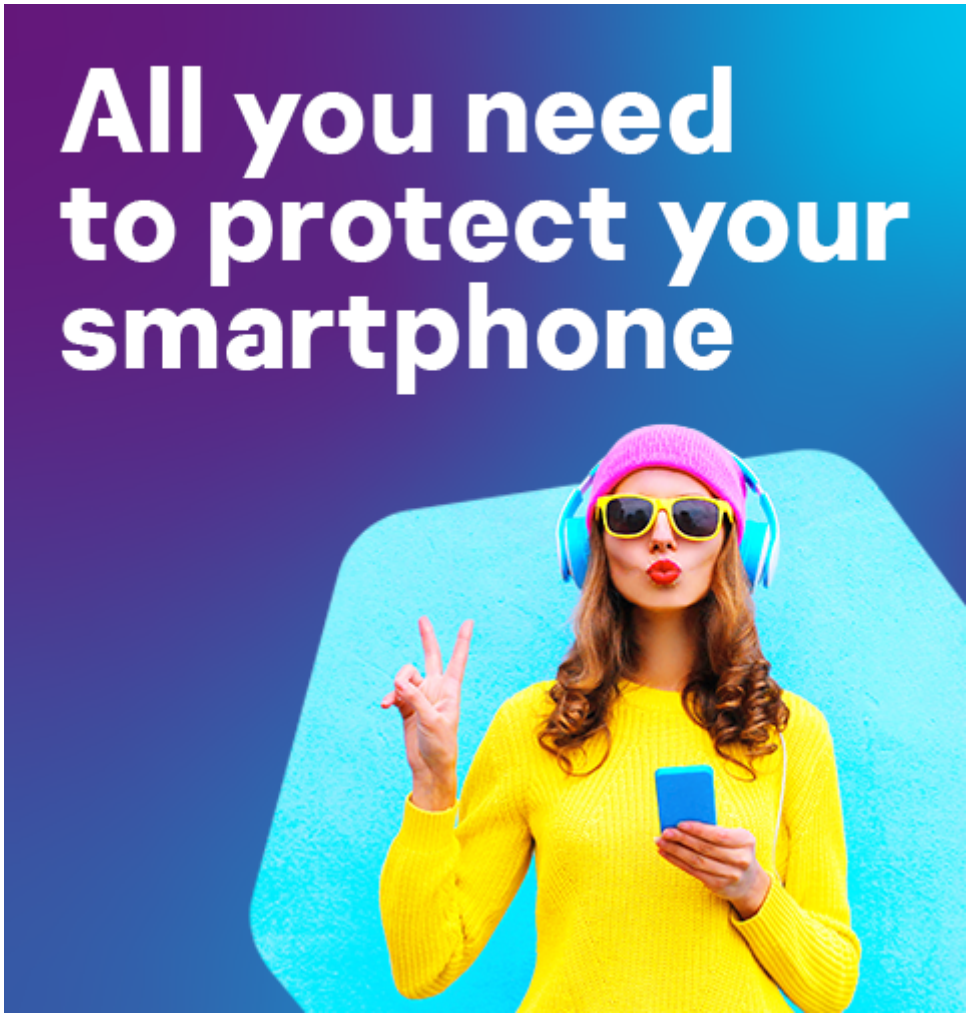
Please let us know what you think about this article

How would you rate this article?

Continue

0days android APT Costin Raiu GReAT iOS mobile devices Pegasus spyware

Share article



Related

EyePyramid: happy-go-lucky malware

↓ Read next

Spectre vulnerability: 4 years after discovery

Does hardware vulnerabilities in CPU pose a practical threat to businesses?

February 2, 2022

Tips

How to avoid online recruitment scams in 2023

Received an attractive job offer from a stranger? Be careful! It could be a scam...

January 24, 2023

Tips

New Year's resolutions for a secure 2023

Six simple steps for personal digital security in 2023.

January 13, 2023

Tips

Cybersecure Christmas

Many hacks have started during Christmas holidays. A few simple tips will reduce the chances of your company becoming the next victim.

December 21, 2022

Tips

Is Avast Safe to Use in 2023?

Avast solutions have a pretty good reputation, but a handful of incidents call their safety into question. Read on to learn whether Avast can be trusted.

December 7, 2022

Email Address

I agree to provide my email address to “AO Kaspersky Lab” to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the “unsubscribe” link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

Home Products

Kaspersky Standard

Kaspersky Plus

Kaspersky Premium

All Products

Small Business Products
1-25 EMPLOYEES

Kaspersky Small Office Security

Kaspersky Endpoint Security Cloud

All Products

Medium Business Products
26-999 EMPLOYEES

Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security for Business Select

Kaspersky Endpoint Security for Business Advanced

All Products

Enterprise Solutions
1000 EMPLOYEES

Cybersecurity Services

Threat Management and Defense

Endpoint Security

Hybrid Cloud Security

All Solutions