IN-DEPTH **PREMIUM REPORTS**

How Hackers Can Control Your Phone Without You Clicking on a Link

Zero-click attacks have evolved from being used to primarily target high-profile people for information to becoming a threat to anyone with a smart device.

Illustration by The Epoch Times, Shutterstock

By Chris Summers | May 18, 2025 Updated: May 18, 2025

In 2025, most people are inseparable from their laptops and smartphones. With that familiarity has come a wariness of the dangers of clicking on unsolicited emails, SMS, or WhatsApp messages.

But there is a new and growing menace called zero-click attacks, which have previously targeted only VIPs or the very wealthy because of their cost and sophistication.

A zero-click attack is a cyberattack that hacks a device without the user clicking anything. It can happen just by receiving a message, call, or file. The attacker uses hidden flaws in apps or systems to take control of the device, with no action needed from the user and the user remains unaware of the attack.

“Although public awareness has increased recently, these attacks have steadily evolved over many years, becoming more frequent as smartphones and connected devices proliferated,” Nathan House, CEO of StationX, a UK-based cybersecurity training platform, told The Epoch Times.

“The key vulnerability is in the software, rather than the type of device, meaning any connected device with exploitable weaknesses could potentially be targeted,” he said.

Aras Nazarovas, an information security researcher at Cybernews, told The Epoch Times why zero-click attacks usually target VIPs, rather than ordinary individuals.

“Since finding such zero-click exploits is difficult and expensive, most of the time such exploits are used to gain access to information from key figures, such as politicians or journalists in authoritarian regimes,” he said.

“They are often used in targeted campaigns. Using such exploits to steal money is rare.”

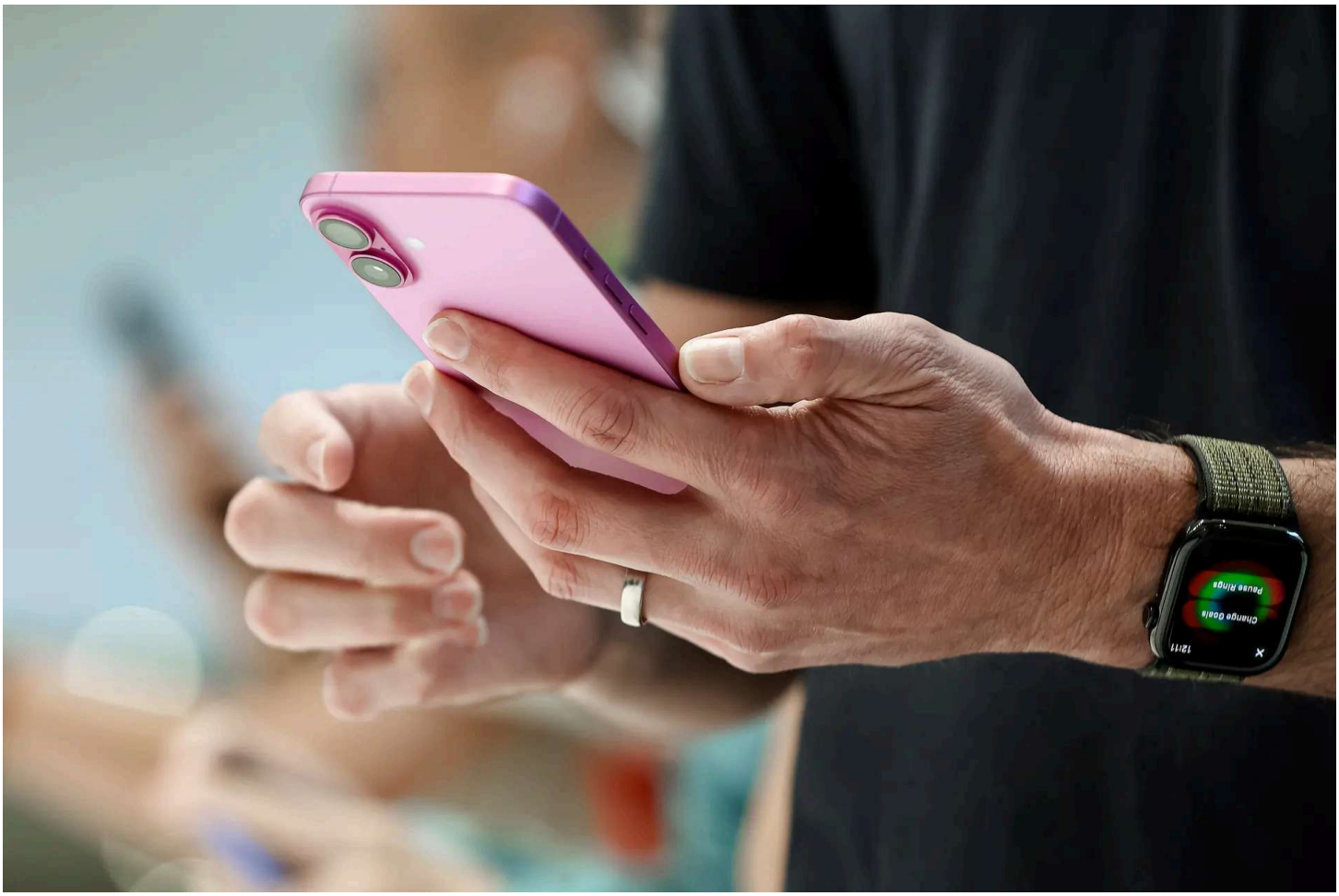
In June 2024, the BBC reported that social media platform TikTok had admitted that a “very limited” number of accounts, including those of media outlet CNN, had been compromised.

> **It has been a billion-dollar market for years, selling zero-click exploits and exploit chains.**
>
> *Aras Nazarovas, information security researcher, Cybernews*

While ByteDance, the owner of TikTok, did not confirm the nature of the hack, cybersecurity companies such as Kaspersky and Assured Intelligence suggested it stemmed from a zero-click exploit.

“The part that requires high levels of sophistication is finding bugs that allow such attacks and writing exploits for these bugs,” Nazarovas said.

“It has been a billion-dollar market for years, selling zero-click exploits and exploit chains. Some gray/dark market exploit brokers often offer $500,000 to $1 million for such exploit chains for popular devices and apps.”



An attendee inspects the new iPhone 16 Pro Max during event at the Apple headquarters in Cupertino, Calif., on Sept. 9, 2024. Experts warn of a rise in zero-click attacks—cyberattacks that compromise devices without any user interaction. Justin Sullivan/Getty Images

Nazarovas added that while ordinary users have been hit in the past by zero-click ‘drive-by’ attacks. These are attacks that emerge after the unintentional installation of malicious software onto a device, often without the user even realizing it. They have become more infrequent with the growing gray market for such exploits.

House said zero-click exploits often seek out vulnerabilities in software and apps that are expensive to discover, which means the perpetrators are usually “nation-state actors or highly-funded groups.”

Expanded Spyware Markets

Although there have been recent innovations in AI that have made certain cyber crimes, such as voice-cloning or vishing, more prevalent,

Nazarovas says there is no evidence yet that it has increased the risk from zero-click attacks.

House said people could use AI to "write zero-click exploit chains for people who would have otherwise lacked the time, experience, or knowledge to be able to discover and write such exploits."

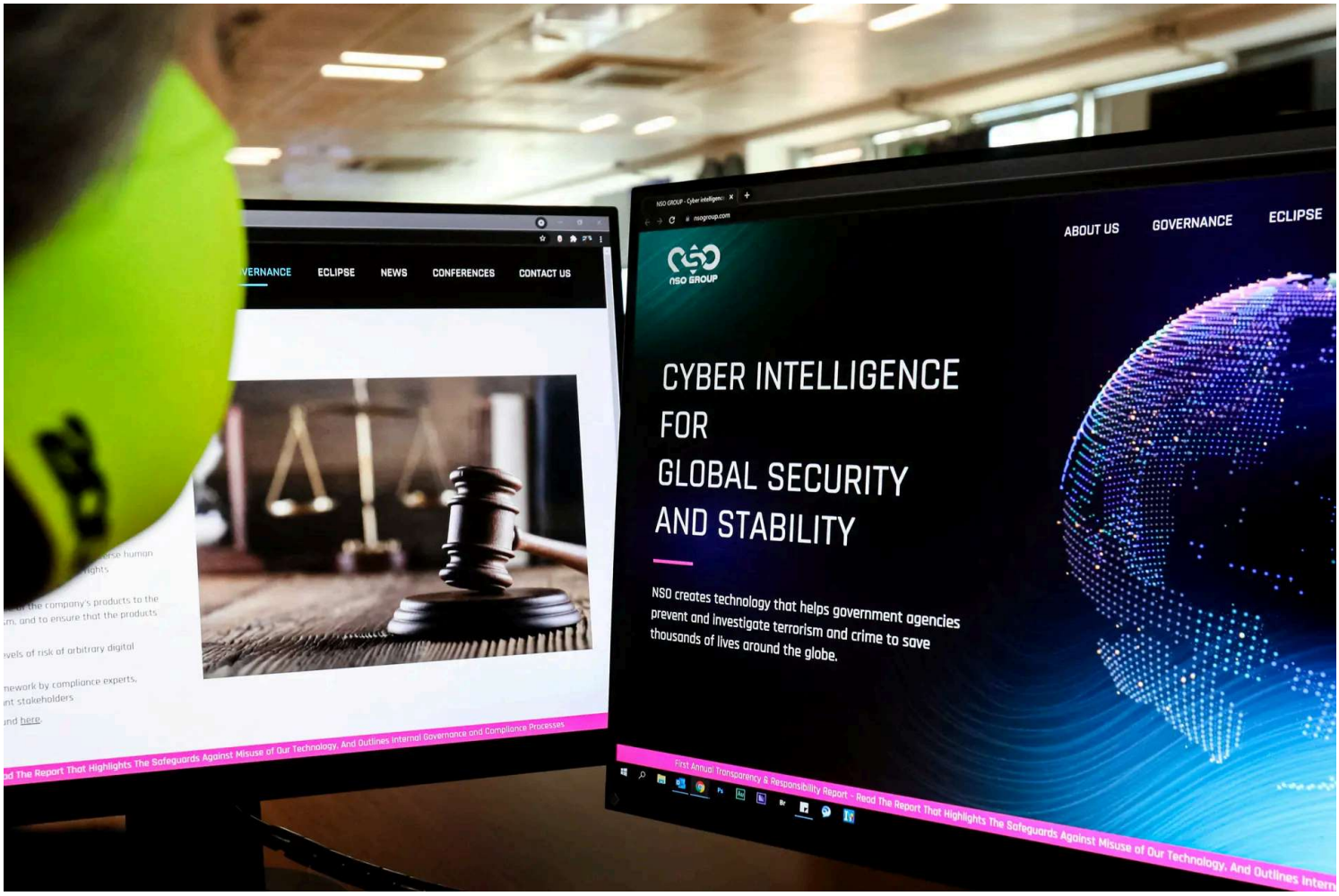
In 2021, The Guardian and 16 other media outlets alleged that foreign governments used Pegasus to surveil at least 180 journalists and other targets worldwide.

But, he said, the increase in zero-click attacks in recent years, "stems mainly from expanded spyware markets and greater availability of sophisticated exploits, rather than directly from AI-driven techniques."

He said zero-click attacks have existed for more than a decade, the most infamous of which was the Pegasus spyware affair.

In July 2021, The Guardian and 16 other media outlets published a series of articles, alleging that foreign governments used the Israeli-based NSO Group's Pegasus software to surveil at least 180 journalists and numerous other targets around the world.

Alleged targets of Pegasus surveillance included French President Emmanuel Macron, Indian opposition leader Rahul Gandhi, and Washington Post writer Jamal Khashoggi, who was slain in Istanbul on Oct. 2, 2018.



A woman checks the website of Israel-made Pegasus spyware at an office in Nicosia, Cyprus, on July 21, 2021. Pegasus has been tied to several high-profile international zero-click attacks in recent years. Mario Goldman/AFP via Getty Images

In a statement at the time, NSO Group said, "As NSO has previously stated, our technology was not associated in any way with the heinous murder of Jamal Khashoggi."

On May 6, a California jury awarded WhatsApp's parent company, Meta, $444,719 in compensatory damages and $167.3 million in punitive damages, in a privacy case against NSO Group.

The WhatsApp complaint was focused on the Pegasus spyware, which, according to the lawsuit, was developed "to be remotely installed and enable the remote access and control of information—including calls, messages, and location—on mobile devices using the Android, iOS, and BlackBerry operating systems."

'Collateral Targets'

How Chinese Imports Are Leveraged in Cyberattacks

US Drone Maker Thrives After Military Bans Chinese Models

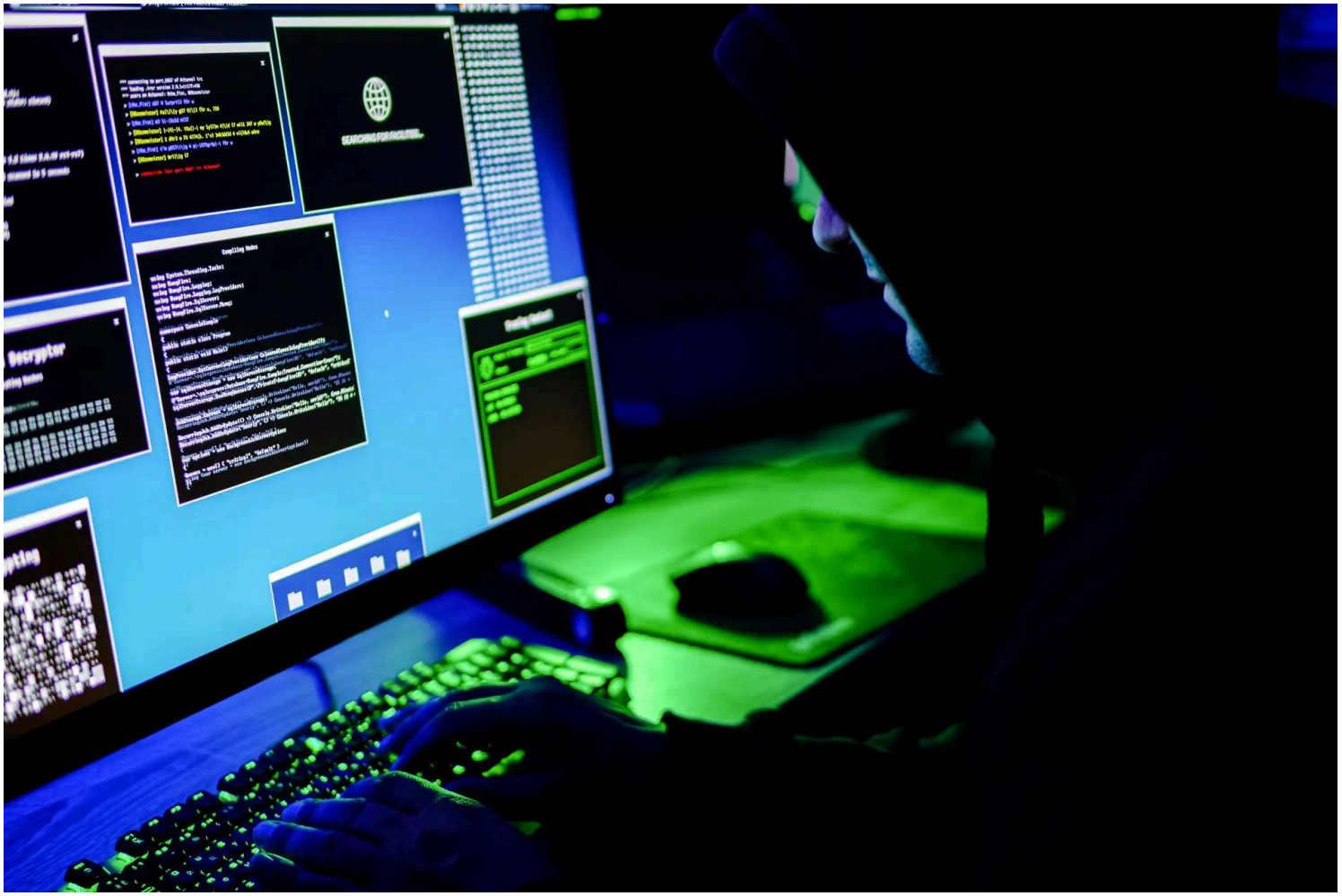
“While ordinary users can occasionally become collateral targets, attackers generally reserve these costly exploits for individuals whose information is especially valuable or sensitive,” Nazarovas said.

According to Nazarovas, corporations offer hackers ‘bug bounties’ to incentivize them to find these exploits and report them to the company, rather than selling them to a broker who then sells them on to parties who use them illegally.

House said defending against zero-click attacks is “challenging,” but some simple cybersecurity steps can reduce the risk.

“Users should always keep software and operating systems updated, regularly reboot their devices, and use hardened security modes such as Apple’s lockdown mode, especially if they believe they’re high-risk targets,” he said.

House said that whatever precautions are taken, it is crucial to recognize “exceptionally sophisticated attacks—like those from advanced nation-state adversaries—can bypass even the most robust defenses.”



In this photo illustration, a hacker types on a computer keyboard on May 13, 2025. Anna Varavva/The Epoch Times

Nazarovas said many big tech players, such as Apple, Google, and Microsoft, collect extensive telemetry data from billions of devices and use the data to detect zero-click exploits and other sophisticated attacks. Telemetry data is information collected remotely from devices such as phones and computers. This data, especially on app usage and behavior, is sent back to a central system to help improve performance, fix problems, or track activity.

“When vulnerabilities that allow such attacks are detected, they can be quickly fixed and rolled out almost immediately to billions of people thanks to automatic updates,” Nazarovas said.

More Premium Reports See More

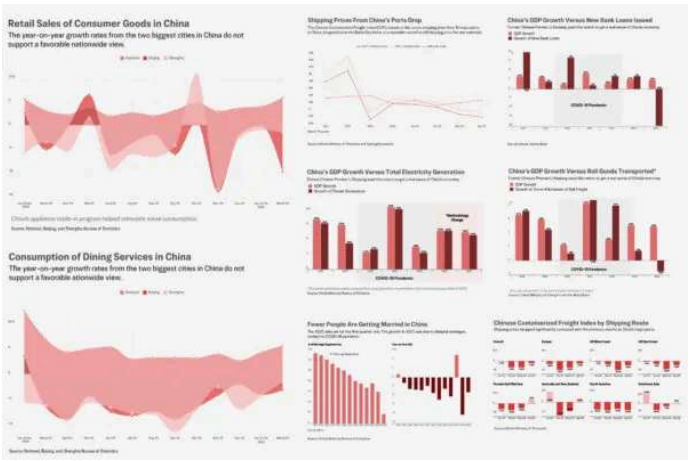
What to Know About the Problems in Newark's Airspace

Greenland's Mineral Wealth Could Pave Way to Independent Future

Even With Trump's Orders, an Uncertain Future for Pennsylvania's Coal Miners

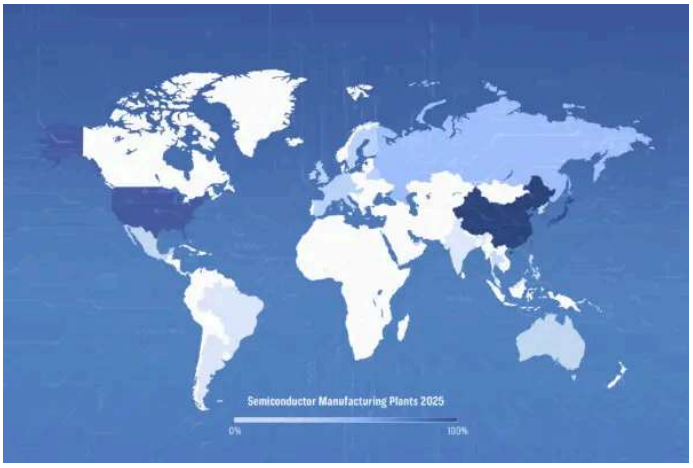
How Legal Immigration Is Keeping Farms Afloat

Parents of Autistic Children Weigh In on RFK Jr.'s Plan to Find the Cause



A Look at China's Economy in 8 Charts

How Falun Gong Spread and Transformed China in the ’90s



Trump Admin Eyes Semiconductor Tariffs—Here’s What to Know

Hollywood Unions Cautiously Welcome Trump’s Movie Tariff Proposal

End of Ranching in Iconic California Community Signals Bigger War on Land Use in West