Since at least late August, sophisticated hackers used flaws in macOS and iOS to install malware on Apple devices that visited Hong Kong–based media and pro-democracy websites. The so-called watering hole attacks cast a wide net, indiscriminately placing a backdoor on any iPhone or Mac unfortunate enough to visit one of the affected pages.

Apple has patched the various bugs that allowed the campaign to unfold. But a report Thursday from Google's Threat Analysis Group shows how aggressive the hackers were and how broadly their reach extended. It's yet another case of previously undisclosed vulnerabilities, or zero-days, being exploited in the wild by attackers. Rather than a targeted attack that focuses on high-value targets like journalists and dissidents, though, the suspected state-backed group went for scale.

The recent attacks specifically focused on compromising Hong Kong websites "for a media outlet and a prominent pro-democracy labor and political group," according to the TAG report. It's unclear how hackers compromised those sites to begin with. But once installed on victim devices, the malware they distributed ran in the background and could download files or exfiltrate data, conduct screen capturing and keylogging, initiate audio recording, and execute other commands. It also made a "fingerprint" of each victims' device for identification.

The iOS and macOS attacks had different approaches, but both chained multiple vulnerabilities together so attackers could take control of victim devices to install their malware. TAG was not able to analyze the full iOS exploit chain, but identified the key Safari vulnerability that hackers used to launch the attack. The macOS version involved exploitation of a WebKit vulnerability and a kernel bug. All were patched by Apple throughout 2021, and the macOS exploit used in the attack was previously presented in April and July conference talks by Pangu Lab.

The researchers emphasize that the malware delivered to targets through the watering hole attack was carefully crafted and "seems to be a product of extensive software engineering." It had a modular design, perhaps so different components could deploy at different times in a multistage attack.

Chinese state-backed hackers have been known to use an extravagant number of zero-day vulnerabilities in watering hole attacks, including campaigns to target Uighurs. In 2019, Google's Project Zero memorably unearthed one such campaign that had gone on for more than two years, and was one of the first public examples of iOS zero days being used in attacks on a broad population rather than specific, individual targets. The technique has been used by other actors as well. Shane Huntley, director of Google TAG, says that the team doesn't speculate about attribution and didn't have enough technical evidence in this case to specifically attribute the attacks. He added only that "the activity and targeting is consistent with a government-backed actor."

"I do think it is notable that we are still seeing these attacks and the numbers of zero-days being found in the wild are increasing," says Huntley. "Increasing our detection of zero-day exploits is a good thing—it allows us to get those vulnerabilities fixed and protect users, and gives us a fuller picture of the exploitation that is actually happening so we can make more informed decisions on how

to prevent and fight it.”

Apple devices have long had a reputation for strong security and fewer problems with malware, but this perception has evolved as attackers have found and exploited more and more zero-day vulnerabilities in iPhones and Macs. As broad watering hole attacks have shown many times now, attackers aren’t just going after specific, high-value targets—they’re ready to take on the masses, no matter what device they own.

More Great WIRED Stories

- ? The latest on tech, science, and more: Get our newsletters!
- Blood, lies, and a drug trials lab gone bad
- *Age of Empires IV* wants to teach you a lesson
- New sex toy standards let some sensitive details slide
- What the new MacBook Pro finally got right
- The mathematics of cancel culture
- ?? Explore AI like never before with our new database
- ? Optimize your home life with our Gear team’s best picks, from robot vacuums to affordable mattresses to smart speakers

Source: **Hackers Targeted Hong Kong Apple Devices in Widespread Attack**