EINPRESSWIRE

iVerify Details First Known Mass iOS Attack

Attack uses sophisticated exploit framework that appears to have been developed by a nation-state

iVerify logo

BELFAST, NORTHERN IRELAND & NEW YORK, NY, UNITED STATES, March 3, 2026 /EINPresswire.com/ -- Today, iVerify announced the results of an investigation into a sophisticated exploit framework, partially detailed by Google Threat Intelligence Group (GTIG). This is the first observed mass exploitation of mobile phones, including iOS, by a criminal group using tools likely built by a nation-state. GTIG refers to UNC6691 using a sophisticated exploit chain developed by a spyware vendor, which iVerify assesses has similarities to previous frameworks developed by threat actors affiliated with the US government. This same framework was also observed by Russian threat actors targeting Ukrainians.

iVerify's research team has reverse engineered the full sample it dubbed CryptoWaters that utilizes the Coruna iOS exploit framework, and developed indicators of compromise (IOC). These IOCs have been deployed within iVerify Enterprise so customers are already protected, as well as to the iVerify Basic app, made free until May for iOS and the next eight days, starting tomorrow, for Android in order to help the public check for infection and take action.

iVerify will be hosting a town hall today, March 3 at 4 p.m. EST to brief the community. Register: iverify.io/events/iverify-mobile-threat-briefing-coruna-mobile-exploit-framework or contact us for a private briefing.

How did this happen?
Despite assurances from commercial spyware developers and the governments who purchase them that use will be limited to counterterrorism, only against criminals and by non-authoritarian administrations, the reality has begun to settle in, once spyware or an exploit capability is sold, control over the end customer is lost. Brokers can't be trusted with these capabilities and business to business transactions over the spyware market are highly unregulated. This lack of control helped launch discussions about responsible use of spyware and aligning on a formal voluntary framework for its use called the Pall Mall Process. While those discussions are ongoing, the economic pressures for spyware companies to return a profit mean

these tools are being sold to a broader array of organizations.

Report after report last year showed that spyware had moved beyond the expected targets in civil society such as journalists and dissidents in addition to criminal operatives, to hit executives in technology and financial services, political campaigns and other people of influence or with privileged access. The more widespread the use, the more certain a leak will occur. While iVerify has some evidence that this tool is a leaked US government framework, that shouldn’t overshadow the knowledge that these tools will find their way into the wild and will be used unscrupulously by bad actors.

We saw this exact scenario occur with EternalBlue, an exploit software for Microsoft Windows developed by the NSA that leveraged a zero-day to let attackers gain access to any number of Windows devices connected to a network. The NSA purposefully did not report the vulnerability to Microsoft, leveraging it for a number of years in its own cyber operations. Unfortunately, shadow brokers stole the exploit and while Microsoft, which was then alerted of the vulnerability, rushed to release a patch, EternalBlue was put up for sale and then publicly released. Two months later, a computer worm burst onto the scene that leveraged the EternalBlue exploit called WannaCry that popped unpatched systems. The same framework was used again to great effect in the NotPetya attacks six weeks after as well as again later that same year for a banking trojan known as Retefe. And that’s exactly what happened again here, but on mobile devices.

“Phone OEMs do as good a job as anyone can do to protect their platforms — alone. But they are also the only platforms that insist on doing it alone. Every other endpoint widely used in enterprise contexts has a robust security framework that allows the collective wisdom of the security community to help keep those endpoints safe,” said Rocky Cole, co-founder and COO at iVerify. “This lack of system data access on phones leaves security teams and users with three options: blindly trust the OEMs, try to build something themselves, or use iVerify Enterprise. While we’re proud of the work we do, people should have choices for how they defend their devices, and it’s long past time for Apple to open up a security framework on iOS. It’s not unprecedented, APIs exist for Macbooks that run macOS software, which is increasingly similar to the iOS operating software.”

While full analysis will take months, shared below are some initial findings about methods of infection, how the malware has been observed to behave as well as some of the traces that it leaves behind while executing these processes in order to help other researchers find compromised devices.

How does a phone become infected?
Spyware attacks are moving from being highly targeted to mass deployment - this campaign is a perfect example. The criminal group is deploying the malware in a watering hole attack mostly targeted at pornography and cryptocurrency sites. From iVerify’s research a portion of the exploit chain was patched with iOS 17.3.

What does this malware do?
This malware silently infects devices and automatically steals cryptocurrency and harvests sensitive data, including photographs and emails. The research found that all crypto wallets other than WhatsApp are vulnerable to this attack.

How can it be detected?
For iVerify Enterprise customers, the app is already tooled to be able to detect infection. For other folks, the recommendation is to download iVerify Basic, which is free for the next month on iOS and the next eight days starting tomorrow on Android, and is also enabled to find IOCs, which are detailed in the company’s technical blog.

If I am impacted, how do I get rid of it?
First and foremost, update devices to the most recent software version which includes the latest patches for known vulnerabilities. Generally, spyware attacks lack persistence meaning that restarting a phone will clear the infection but a device can be reinfected if the user visits one of the malicious sites again. While it can be a pain, restarting your device daily is currently the best defense against advanced malware for people who don’t have access to mobile security teams or a comprehensive mobile security platform like iVerify Enterprise. We also recommend resetting passwords for any online services accessed from your device and enabling two-factor authentication on all critical accounts.

For the full technical analysis visit the iVerify blog. To download iVerify Basic visit the App Store on iOS and the Play Store on Android.

To learn more about iVerify Enterprise visit www.iverify.com.

About iVerify

iVerify is a pioneer in mobile endpoint detection and response (EDR) solutions, providing advanced protection against the real threats mobile devices face. The company's comprehensive security platform safeguards organizations from fileless malware, smishing, malicious applications, ransomware operations, and breaches resulting from credential theft. iVerify's solutions span from consumer to enterprise and government sectors, offering both privacy-focused BYOD protection and enterprise-grade security capabilities to ensure every device in the workplace is secure.

For more information, please visit www.iverify.com.

Monika Hathaway
iVerify
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/897269335