iVerify Mobile Threat Investigation Uncovers New Pegasus Samples

Published: 2024-12-04 · Archived: 2026-04-05 14:54:20 UTC

For years, our understanding of mobile device threats was built on a dangerously narrow foundation. Mobile malware investigations were limited to a microscopic sample of devices – typically those belonging to high-risk targets like journalists, political activists, and government officials. These early investigations were critical to helping the world understand a new wave of capability, but their limited nature still leaves a massive blind spot to understanding the scope of mobile device compromise.

Imagine trying to understand an entire ocean by examining a single teaspoon of water. That was the state of mobile device security research. Investigations were expensive, time-consuming, and accessible only to a privileged few with specialized forensic skills and significant resources. Each study might involve just a handful of devices, often pre-selected because they were already suspected of being compromised.

The result? A fundamentally skewed perception of mobile device security. Spyware like Pegasus was treated as a rare, targeted threat – something that might impact a member of civil society, a high-level executive, or a political representative, but surely not an average business professional or everyday smartphone user. We told ourselves comfortable stories about the rarity of these threats without ever truly looking.

Our approach at iVerify was simple but revolutionary: What if we could democratize mobile threat hunting? What if we could allow every smartphone user the ability to conduct a professional-grade security scan in just five minutes?

In May 2024, we did exactly that.

iVerify launched its Mobile Threat Hunting feature, conducting an investigation that would reveal critical insights into the current mobile device security landscape. Our initial investigation consisted of 2,500 self-scanned devices from our user base and resulted in new detections of the now infamous Pegasus mobile spyware.

Democratizing Mobile Threat Detection: An Unexpected Journey

When we launched our Mobile Threat Hunting feature we had no idea we were about to challenge everything the tech world thought it knew about mobile security. We created a solution that put powerful threat detection directly into users' hands – a full mobile threat hunt scan completed in just five minutes, right on their smartphone.

What happened next was nothing short of remarkable. As part of the feature launch, we gave our users the option to conduct a one-time threat hunt of their device via our iVerify application. To our surprise, without a single advertisement, 2,500 of our users jumped at the chance to scan their devices. (Note: If you are a current iVerify app user, you can still complete this threat hunt. If not, download the app today and scan your device). The results of those scans validated what we already assumed: if you scan for it, you will find it. **We uncovered seven**

Pegasus infections – a number that might seem small, but represents a massive red flag in the world of mobile security.

These weren't just recent infections. Our analysis revealed a complex timeline of compromise: one exploit from late 2023 on iOS 16.6, another potential Pegasus infection in November 2022 on iOS 15, and five older infections dating back to 2021 and 2022 across iOS 14 and 15. Each of these represented a device that could have been silently monitored, its data compromised without the owner's knowledge.

The discovery supported our thesis about the prevalence of spyware on mobile devices – it was hiding in plain sight, undetected by traditional endpoint security measures.

Our investigation detected 2.5 infected devices per 1,000 scans – a rate significantly higher than any previously published reports. **However, it's crucial to understand the context of this data:**

- **Targeted Scanning**: These 2,500 devices represent populations most likely to be targeted by advanced spyware
- **Not a Global Representation**: This sample is not indicative of iVerify's entire device population
- **High-Risk Focus**: Devices belonged to journalists, government officials, and corporate executives.

The findings revealed a critical truth: we can only understand the real scope of mobile threats by looking closely. By democratizing malware detection, we're not just protecting devices – we're shining a light into the darkest corners of mobile security, giving users the power to understand and defend against threats that were previously invisible.

This wasn't just a technical achievement. It was a fundamental shift in how we approach mobile security – putting power back into the hands of users, one five-minute scan at a time.

Understanding Pegasus: A Sophisticated Surveillance Tool

Developed by NSO Group, or Rainbow Ronin, as referred to by the iVerify team, Pegasus represents the pinnacle of invasive spyware technology:

- **Complete Device Control**: Access to messages, emails, call logs, photos
- **Zero-Click Attacks**: Infection without user interaction
- **Operating System Vulnerabilities**: Exploits in iOS and Android

iVerify Research Discoveries

Our May 2024 investigation uncovered multiple Pegasus variants:

- 5 unique malware types across iOS and Android
- Forensic artifacts detected in:
    - Diagnostic data

- Shutdown logs
- Crash logs

I will be presenting a deep dive into the Pegasus sample this Friday at OBTS v7.0, if you are not attending in person, the session will be live streamed. I will also publish a technical blog post in the coming weeks dissecting the sample and sharing it with industry.

Why Mobile Threat Hunting Matters

Traditional security models fail to capture the nuanced threats facing mobile devices. In the past, Pegasus detections have been rare due to a lack of effective detection solutions, but with improved detection and remediation methods, we believe there is more compromise than is currently understood.

Powers said it best “You can’t see what you don’t understand. But what you think you already understand, you’ll fail to notice.” As an industry, we believe that mobile device security is good enough, but if we took the moment to look at the devices we would likely realize that the threat is far worse than we thought.

The good news, we have built the capability to do this at scale and in a privacy preserving way. Our investigations reveal a critical truth: we cannot understand the scope of mobile threats until we look closely. iVerify is committed to bringing these hidden dangers into the light, protecting individuals and organizations in an increasingly complex digital landscape.

iVerify offers an advanced mobile EDR solution that combines threat detection and mobile forensics with automated response and remediation for enterprise-level protection against sophisticated threats, including mobile malware, unpatched vulnerabilities, smishing, and credential theft, ensuring maximum privacy and security. Take control of your mobile security. Request a demo to experience our advanced capability firsthand.

iVerify also offers special protection at https://iverify.org/ for journalists and civil society.

A Note: iVerify’s Adversary Naming Conventions

iVerify has taken the important step of naming several spyware adversaries we are tracking, addressing a gap in adversary naming that exists today. The NSO Group is referred to by iVerify’s research team as Rainbow Ronin.

When naming, we utilized the traditional threat naming conventions and methodology. We strive to psychologically ensure that adversaries do not appear to be superhuman and, therefore, beatable. We have chosen Ronin, a samurai who had no lord or master, to depict surveillanceware. The comparison is apt as they are a combination of excellent coders and will sell to just about anyone with enough money even though they claim to only sell to nation-states or law enforcement agencies. In keeping with the psychological aspect of naming, we made the decision to mix Ronin with the soft side of a children’s cartoon character (image ponies, rainbows and butterflies). In this spirit, we are naming the NSO Group, Rainbow Ronin to help personify the threat, enhance the ability to conceptualize the risks in the threat landscape and understand the attack methods.

Take Action: Protect Your Mobile Ecosystem

Source: https://iverify.io/blog/iverify-mobile-threat-investigation-uncovers-new-pegasus-samples