# Godfather Banking Trojan Spawns 1.2K Samples Across 57 Countries

By Nate Nelson

Published: 2024-04-25 · Archived: 2026-04-05 21:05:55 UTC

3 Min Read

Source: Wodthikorn Phutthasatchathum via Alamy Stock Photo

North of 1,000 samples of the Godfather mobile banking Trojan are circulating in dozens of countries worldwide, targeting hundreds of banking apps.

First discovered in 2022, Godfather — which can record screens and keystrokes, intercepts two-factor authentication (2FA) calls and texts, initiates bank transfers, and more — has quickly become one of the most widespread malware-as-a-service offerings in cybercrime, especially mobile cybercrime. According to Zimperium's 2023 "Mobile Banking Heists Report," as of late last year, Godfather was targeting 237 banking apps spread across 57 countries. Its affiliates exfiltrated stolen financial information to at least nine countries, primarily in Europe and including the US.

All that success drew attention, so, to prevent security software from spoiling the party, Godfather's developers have been automatically generating new samples for their customers at a near industrial scale.

Other mobile malware developers across the spectrum have started doing the same thing. "What we're seeing is that malware campaigns are starting to get bigger and bigger," warns Nico Chiaraviglio, chief scientist at Zimperium, who will host a session on this and other mobile malware trends at RSAC in May.

Besides Godfather and other known families, Chiaraviglio is tracking an even bigger, still-under-wraps mobile malware family with more than 100,000 unique samples in the wild. "So that's crazy," he says. "We haven't seen that number of samples in a single malware before, ever. This is definitely a trend."

## Banking Trojans Spawn Hundreds of Samples

Mobile security is already lagging far behind security for desktops. "In the '90s, no one was really using antivirus on desktop computers, and that's kind of where we are now. Today, only one of four users are really using some sort of mobile protection. Twenty-five percent of devices are completely unprotected, compared with desktop, at 85%," Chiaraviglio laments.

Mobile threats, meanwhile, are leveling up fast. One way they're doing so is by generating so many different iterations that antivirus programs — which profile malware by their unique signatures — have trouble correlating one infection with the next.

Consider that at the time of its initial discovery in 2022, according to Chiaraviglio, there were fewer than 10 samples of Godfather in the wild. By the end of last year, that number had risen a hundredfold.

Its developers have clearly been autogenerating unique samples for customers to help them avoid detection. "They could just be scripting everything — that would be a way to automate it. Another way would be to use large language models, as code assistance can really speed up the development process," Chiaraviglio says.

Other banking Trojan developers have followed the same approach, if at a lesser scale. In December, Zimperium tallied 498 samples of Godfather's close competitor, Nexus, 300 samples of Saderat, and 123 of PixPirate.

## Can Security Software Keep Up?

Security solutions that tag malware by signature will find difficulty keeping track of hundreds and thousands of samples per family.

"Maybe there is a lot of code reuse between different samples," Chiaraviglio says, something he suggests adaptive solutions can use to correlate related malware with different signatures. Alternatively, instead of the code itself, defenders can use artificial intelligence (AI) to focus on the behaviors of the malware. With a model that can do that, Chiaraviglio says, "it doesn't really matter how much you change the code or the way the application looks, we will still be able to detect it."

But, he admits, "at the same time, this is always a race. We do something [to adjust], then the attacker does something to evolve to our predictions. [For example], they can ask [a large language model] to mutate their code as much as it can. This would be the realm of polymorphic malware, which is not something that happens a lot on mobile, but we might start seeing way more of that."

## About the Author

Contributing Writer

Nate Nelson is a journalist and scriptwriter. He writes for "Darknet Diaries" — the most popular podcast in cybersecurity — and co-created the former Top 20 tech podcast "Malicious Life." Before joining Dark Reading, he was a reporter at Threatpost.

---