

Forum:[Hack Forums](#)

Thread: [The Rise of RatOn: From NFC heists to remote control and ATS](#)

MadScientist - September 14, 2025, 9:54 pm

Remote Access Trojans (RATs) are a popular commodity on the dark web, particularly when offering full remote control of infected devices. Key features typically sought after include visual access to the device's screen (in other words: screen casting), as well as a text-based interface that presents a pseudo-screen with textual descriptions of on-screen elements. The latter method offers more responsive and efficient control, as transmitting text consumes significantly fewer resources than streaming graphical data.

While the concept of combining a RAT with an NFC relay attack isn't entirely new, documented cases are rare. Instances where a trojan evolves from a basic NFC relay tool into a sophisticated RAT with Automated Transfer System (ATS) capabilities are virtually unheard of. That's why the discovery of the new trojan RatOn by ThreatFabric MTI analysts is particularly noteworthy. RatOn merges traditional overlay attacks with automatic money transfers and NFC relay functionality—making it a uniquely powerful threat.

While monitoring the NFSkate threat actor group activity, we came across a quite unique sample. What separated this sample from previous ones was the fact that it was not just a standalone APK file, but it was a part of a campaign involving more unique applications.

Our analysis of the campaign revealed a new fully functional banking trojan with device/account takeover capabilities, targeting cryptocurrency wallet applications. Besides that, the malware can perform automated money transfers abusing one specific bank application, as well as perform ransom using custom overlay pages and device locking.

In this report we will uncover the details about this previously unreported trojan which we dubbed as RatOn, based on the name threat actors used for group chat where their discussed the malware. We guess that RAT in the group name refers to Remote Access Tool or Trojan.

According to our telemetry the first related sample was assembled on 5th of July 2025 and the latest on 29th of August 2025. It means that threat actor group focusing on new malware developments for at least two months already. Some of the related samples still have minor detections on VirusTotal

Attackers registered domains with adult themes to infect victims. Such a domains contained TikTok18+ inside their name and directly hosted the malicious dropper application. There is no certainty on how exactly the attackers lure victims to visit such web sites. So far, we know that those pages targeted Czech and Slovakian speaking auditory.

Source -

<https://www.threatfabric.com/blogs/the-rise-of-raton-from-nfc-heists-to-remote-control-and-ats>