New NFC-Based PhantomCard Malware Targets Android Banking Users - A

Data: 2025-08-15 01:31:49

Autor: Inteligência Against Invaders

ThreatFabric analysts have uncovered PhantomCard, a sophisticated NFC-based Trojan designed to relay sensitive card data from victims' devices to cybercriminals.

This malware, which primarily targets banking customers in Brazil but shows potential for global expansion, exemplifies the growing interest among threat actors in NFC relay attacks.

PhantomCard operates by masquerading as a legitimate "card protection" app, distributed through deceptive web pages mimicking the Google Play Store.

Once installed, it requires no additional permissions, immediately prompting users to tap their physical banking cards against the infected device for supposed verification.

This action initiates the relay of NFC data via a criminal-controlled server, enabling fraudsters to perform unauthorized transactions at point-of-sale (POS) terminals or ATMs as if they held the victim's card.

PhantomCard's core functionality hinges on exploiting the NFC reader in modern Android devices, focusing on the ISO-DEP (ISO 14443-4) protocol standard used in EMV contactless cards.

Upon detecting a card, the malware sends specific Application Protocol Data Units (APDUs), such as the SELECT command for the "2PAY.SYS.DDF01" Payment System Environment directory, to confirm it's an EMV-compatible card and extract metadata about available payment applications.

If successful, the data is forwarded to a command-and-control (C2) server, alerting attackers that the card is ready for exploitation.

The malware then facilitates a bidirectional relay: transaction instructions from the fraudster's side are parsed and forwarded to the victim's card, while responses are sent back, effectively bridging the physical card to a remote POS or ATM.

To complete high-value transactions, PhantomCard tricks victims into entering their PIN, which is relayed for authentication.

This setup, demonstrated in actor-shared videos, allows seamless fraud where the victim unwittingly enables payments from afar.

Roots in Malware-as-a-Service

Tracing its origins, PhantomCard is not an original creation but a customized variant of the Chineseorigin “NFU Pay” Malware-as-a-Service (MaaS) platform, akin to other underground tools like SuperCardX and KingNFC.

Analysis reveals Chinese debug messages and package references to NFU Pay, indicating that the Brazil-based threat actor, known as “Go1ano developer,” acquired and rebranded it for local distribution.

This actor, a “serial reseller” of Android threats, promotes PhantomCard as “GHOST NFC CARD” on Telegram, targeting Brazilian mobile banking users while claiming global adaptability.

Indicators such as the C2 endpoint “/baxi/b” (Chinese for “Brazil”) suggest region-specific tailoring, raising alarms about potential variants for other markets.

The reseller model underscores a shift in the cyber threat landscape, where non-technical actors act as local distributors, bridging global MaaS offerings to regional underground markets.

“Go1ano developer” also resells families like BTMOB and GhostSpy, and recently transferred rights to “Pegasus Team,” linked to other Brazilian Trojans like Rocinante.

This outsourcing expands the reach of sophisticated threats, bypassing language and cultural barriers, and complicates defenses for financial institutions.

Mitigation Strategies

PhantomCard highlights the surging demand for NFC relay tools, building on precursors like NFCGate and NFSkate, but with a streamlined, EMV-focused implementation using libraries like “scuba_smartcards” for data parsing.

For banks, such malware poses detection challenges, as transactions appear legitimate originating from the victim’s physical card with PIN confirmation leaving only anomalies like mismatched merchant locations as red flags.

ThreatFabric recommends vigilant monitoring of similar families, user education against apps requesting card taps for “protection,” and enhanced transaction analytics to spot relay fraud.

As MaaS evolves into resold services, global financial organizations must track these actors to safeguard against escalating mobile threats.

Indicators of Compromise

App Name	Package Name	SHA256 Hash
Proteção Cartões	com.nfupay.s145	a78ab0c38fc97406727e48f0eb5a803b1edb9da4a39e613f013b3c5b4736262f
Proteção Cartões	com.rc888.baxi.English	cb10953f39723427d697d06550fae2a330d7fff8fc42e034821e4a4c55f5a667