SpyAgent malware targets crypto wallets, stealing screenshots

By Doug Bonderud

Published: 2024-11-08 · Archived: 2026-04-05 18:24:34 UTC

A new Android malware strain known as SpyAgent is making the rounds — and stealing screenshots as it goes. Using optical character recognition (OCR) technology, the malware is after cryptocurrency recovery phrases often stored in screenshots on user devices.

Here's how to dodge the bullet.

Attackers shooting their (screen) shot

Attacks start — as always — with phishing efforts. Users receive text messages prompting them to download seemingly legitimate apps. If they take the bait and install the app, the SpyAgent malware gets to work.

Its target? Screenshots of the 12-24-word recovery phrases used for cryptocurrency wallets. Since these phrases are too long to easily remember, users often take screenshots for future reference. If attackers compromise these screen captures, they can recover crypto wallets to the device of their choosing, allowing them to steal all the digital currency they contain. And once funds are gone, they're gone — the nature of cryptocurrency protocols means that when transactions are completed, they can't be reversed. If money is sent to the wrong address, senders must ask recipients to create and complete a return transaction.

If users screenshot their recovery phrase and have it stolen by SpyAgent, attackers need only recover the wallet and transfer funds to the destination of their choice.

The malware has been making the rounds in South Korea, with more than 280 APKs affected, according to Coin Telegraph. These applications are distributed outside the official Google Play store, often using SMS messages or social media posts to capture user interest. Some of the infected apps mimic South Korean or UK government services, while others appear to be dating or adult content applications.

There are also indications that attackers may be preparing to expand into the United Kingdom, which could, in turn, lead to more widespread compromise. And while the malware is currently Android-only, there are signs that an iOS version may be in development.

Beyond cryptocurrency: Potential risks of sneaky screenshot steals

While cryptocurrency recovery phrases are the top priority for SpyAgent, using OCR tech means that any picture is up for grabs. For example, if business devices have screenshots of usernames and passwords for databases or analytics tools, company assets could be at risk. Consider a manager with access to multiple secure services, each requiring a unique password to help reduce compromise risk. In an effort to keep passwords safe but still have them available on-demand, our well-meaning manager makes a list and takes a screenshot of their different

credential combinations. Because they believe their device is secure, the company is using solutions such as multi-factor authentication (MFA) and secure single sign-on (SSO), and they don't see their screenshot as a risk.

If hackers convince them to click through and download infected applications, however, attackers can view and steal saved image data and then use this data to "legitimately" gain account access.

Another potential risk comes from personal data. Users may have screenshots of personal health or financial data, which puts them at risk of data exfiltration and identity fraud. They might also have confidential contact details for business partners or executives, opening the door to another round of phishing attacks.

This picture-based approach to compromise creates two problems for security teams. First is the time required for detection. It takes businesses 258 days on average to detect and contain an incident, as noted by the IBM 2024 Cost of a Data Breach Report. But this number only applies if security is firing on all cylinders. If mobile devices are compromised by user actions, and the malware's sole purpose is to find and steal screenshots, the issue could go unnoticed for far longer, especially if attackers bide their time.

Once criminals make the move to strike, meanwhile, the damage may be significant. Using stolen credentials, attackers can gain access to critical services and lockout account owners. From there, they can capture and exfiltrate data across a host of IT systems and services. While this direct action will alert IT teams, security response is naturally reactionary, meaning companies can't avoid the attack; they mitigate the damage.

The message here is simple: If it's on your phone, it's never entirely safe. Screenshots of crypto recovery passwords, corporate logins and passwords or personal data such as Social Security numbers or bank account details are valuable targets for attackers.

Dodging the bullet also means not taking the bait — don't respond to unsolicited texts and only download apps through approved app stores. It also means taking precautions. The always-connected nature of devices means that complete safety is an illusion. The less stored on a device, the better.

Users can keep devices safe by sticking to the official Google Play Store. Applications downloaded outside of the Play Store come with no guarantees about their safety or security. Some are benign apps that haven't passed Google's screening process. Others are near-duplicates of official applications that contain hidden files or commands. And some are simply vehicles to install malware and connect with command and control (C2) servers.

In addition, companies can benefit from the deployment of security automation and AI security tools. These solutions are capable of capturing and correlating patterns of behavior that may appear benign but are collective indicators of compromise (IoCs). As noted by IBM data, businesses that extensively used AI and automation were able to detect and contain breaches 98 days faster than the global average.

The SpyAgent malware is now skulking around South Korea, stealing screenshots to capture crypto recovery passwords, and putting companies at risk of larger-scale data compromise.

The best defense? A trifecta of sparing screenshot saves, suspicion about off-brand apps and the deployment of superior intelligence solutions.
