A new era in mobile banking Trojans

By Roman Unuchek

Published: 2017-07-31 · Archived: 2026-04-05 12:53:47 UTC

In mid-July 2017, we found a new modification of the well-known mobile banking malware family Svpeng – Trojan-Banker.AndroidOS.Svpeng.ae. In this modification, the cybercriminals have added new functionality: it now also works as a keylogger, stealing entered text through the use of accessibility services.

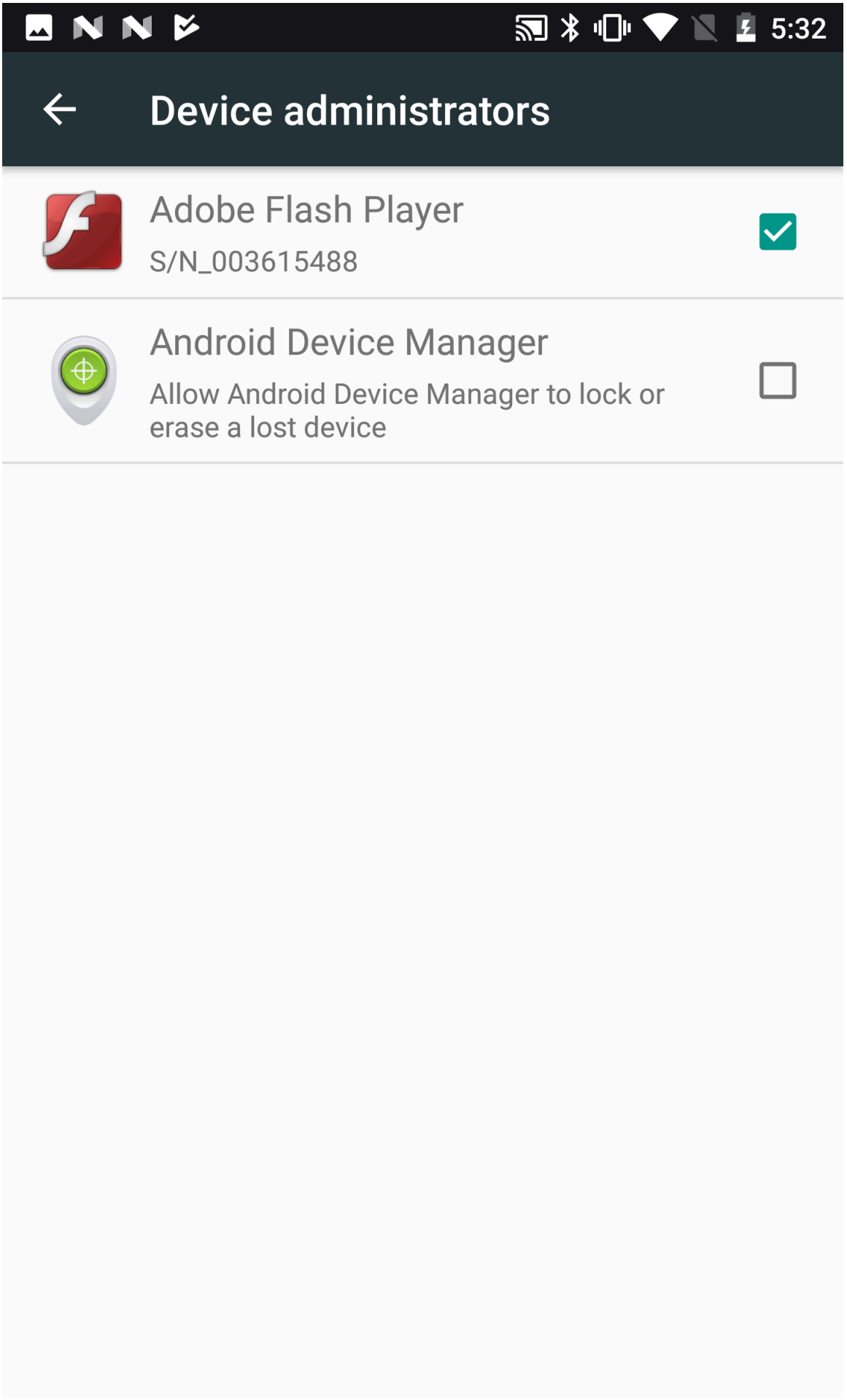
Accessibility services generally provide user interface (UI) enhancements for users with disabilities or those temporarily unable to interact fully with a device, perhaps because they are driving. Abusing this system feature allows the Trojan not only to steal entered text from other apps installed on the device, but also to grant itself more permissions and rights, and to counteract attempts to uninstall the Trojan.

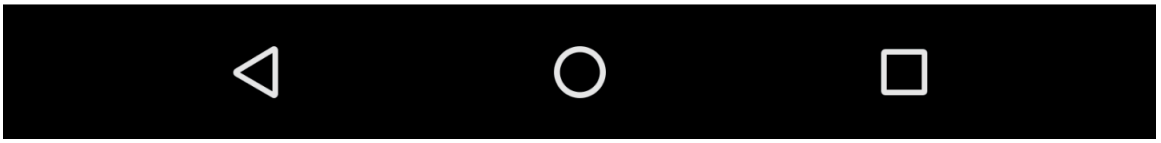
Attack data suggests this Trojan is not yet widely deployed. In the space of a week, we observed only a small number of users attacked, but these targets spanned 23 countries. Most attacked users were in Russia (29%), Germany (27%), Turkey (15%), Poland (6%) and France (3%). It is worth noting that, even though most attacked users are from Russia, this Trojan won't work on devices running the Russian language. This is a standard tactic for Russian cybercriminals looking to evade detection and arrest.

The Svpeng malware family is known for being innovative. Starting from 2013, it was among the first to begin attacking SMS banking, to use phishing pages to overlay other apps to steal credentials, and to block devices and demand money. In 2016, cybercriminals were actively distributing Svpeng through AdSense using a vulnerability in the Chrome browser. This makes Svpeng one of the most dangerous mobile malware families, and it is why we monitor the functionality of new versions.

The attack process

After starting, the Trojan-Banker.AndroidOS.Svpeng.ae checks the device language and, if it is not Russian, asks the device for permission to use accessibility services. In abusing this privilege, it can do many harmful things. It grants itself device administrator rights, draws itself over other apps, installs itself as a default SMS app, and grants itself some dynamic permissions that include the ability to send and receive SMS, make calls, and read contacts. Furthermore, using its newly-gained abilities the Trojan can block any attempt to remove device administrator rights – thereby preventing its uninstallation. It is interesting that in doing so it also blocks any attempt to add or remove device administrator rights for any other app too.


5:32
Device administrators
Adobe Flash Player
S/N_003615488
Android Device Manager
Allow Android Device Manager to lock or erase a lost device



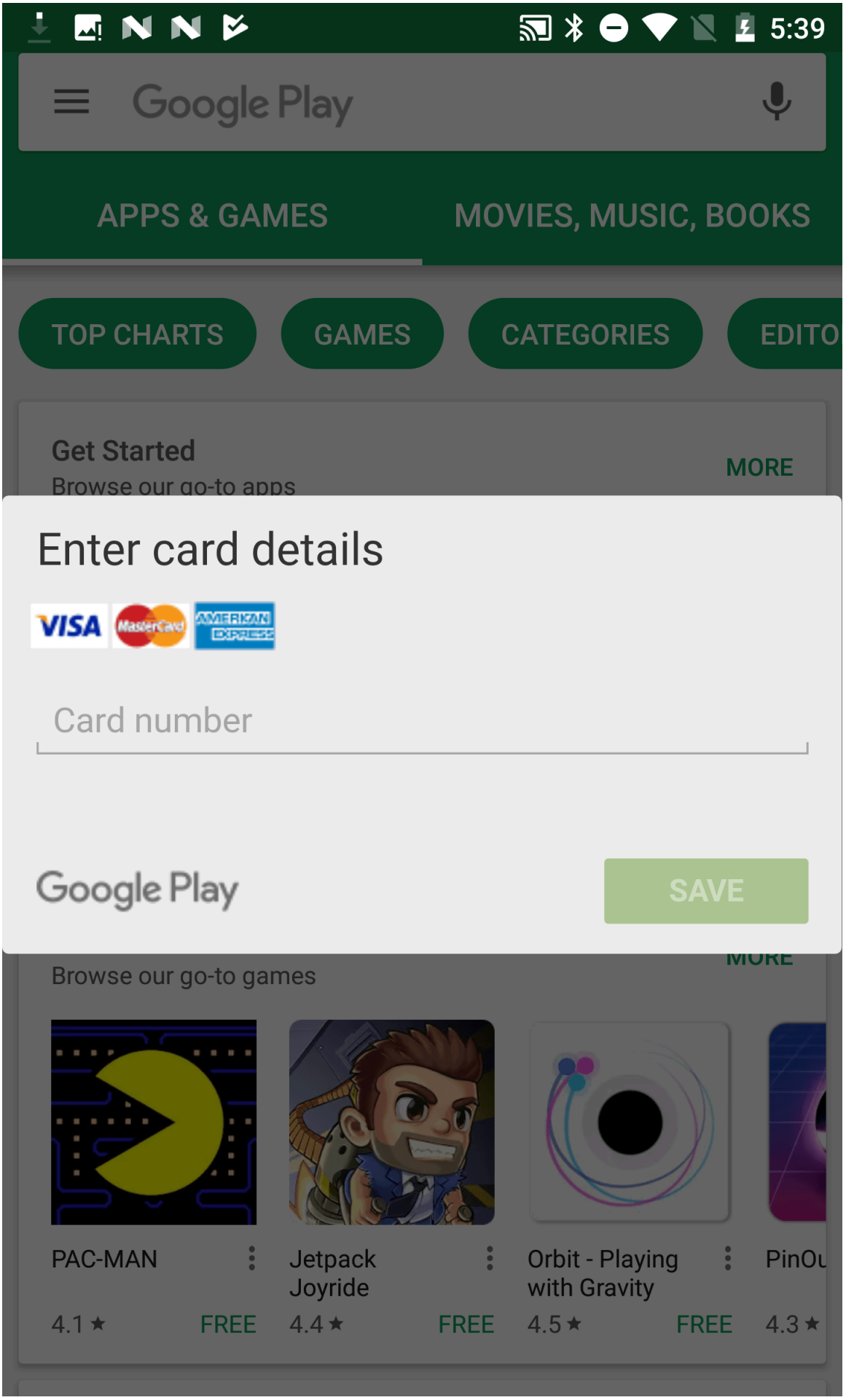
Svpeng was able to become a device administrator without any interaction with the user just by using accessibility services.

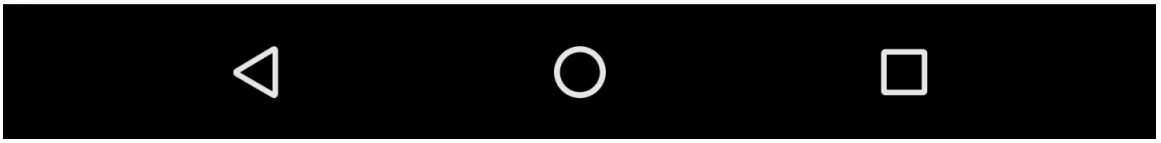
Using accessibility services allows the Trojan to get access to the UI of other apps and to steal data from them, such as the names of the interface elements and their content, if it is available. This includes entered text. Furthermore, it takes screenshots every time the user presses a button on the keyboard, and uploads them to the malicious server. It supports not only the standard Android keyboard but also a few third-party keyboards.

Some apps, mainly banking ones, do not allow screenshots to be taken when they are on top. In such cases, the Trojan has another option to steal data – it draws its phishing window over the attacked app. It is interesting that, in order to find out which app is on top, it uses accessibility services too.

From the information Svpeng receives from its command and control server (CnC), I was able to intercept an encrypted configuration file and decrypt it to find out the attacked apps, and to obtain a URL with phishing pages.

I uncovered a few antivirus apps that the Trojan attempted to block, and some apps with phishing URLs to overlay them. Like most mobile bankers, Svpeng overlays some Google apps to steal credit card details.

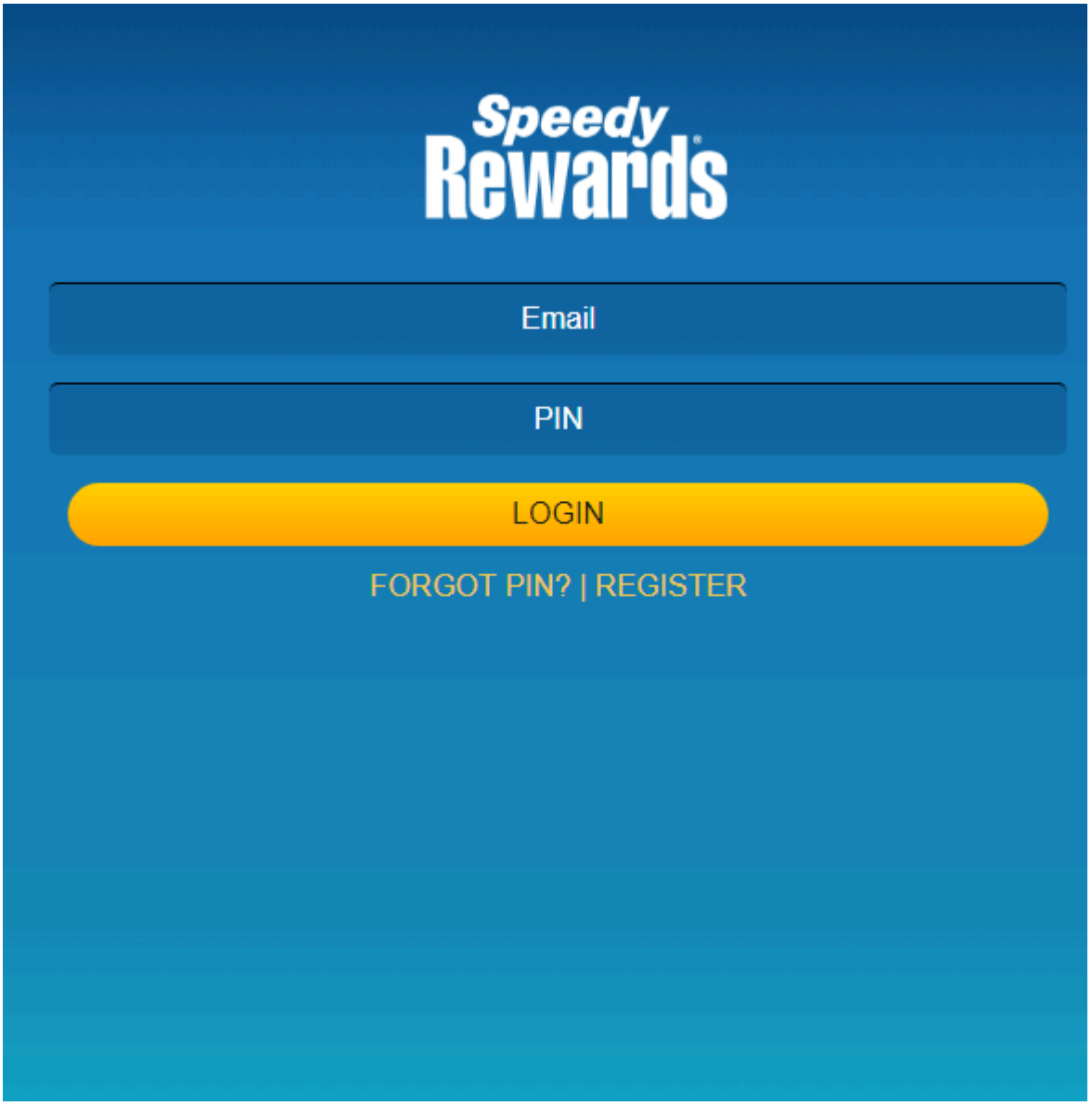

5:39
Google Play
APPS & GAMES
MOVIES, MUSIC, BOOKS
TOP CHARTS
GAMES
CATEGORIES
EDITO
Get Started
Browse our go-to apps
MORE
Enter card details
VISA
MasterCard
AMERICAN EXPRESS
Card number
Google Play
SAVE
Browse our go-to games
MORE
PAC-MAN
4.1 ★
FREE
Jetpack Joyride
4.4 ★
FREE
Orbit - Playing with Gravity
4.5 ★
FREE
PinOu
4.3 ★



Also, the config file contained a phishing URL for the PayPal and eBay mobile apps to steal credentials and URLs for banking apps from different countries:

- UK– 14 attacked banking apps
- Germany – 10 attacked banking apps
- Turkey– 9 attacked banking apps
- Australia– 9 attacked banking apps
- France– 8 attacked banking apps
- Poland– 7 attacked banking apps
- Singapore– 6 attacked banking apps

There was one more app in this configuration file – Speedway app, which is a rewards app, not a financial app. Svpeng will overlay it with a phishing window to steal credentials.



It can also receive commands from the CnC:

- To send SMS
- To collect info (Contacts, installed apps and call logs)
- To collect all SMS from the device
- To open URL
- To start stealing incoming SMS

Distribution and protection

The Trojan-Banker.AndroidOS.Svpeng.ae is distributed from malicious websites as a fake flash player. Its malicious techniques work even on fully-updated devices with the latest Android version and all security updates installed. By accessing only one system feature this Trojan can gain all necessary additional rights and steal lots of data.

MD5

F536BC5B79C16E9A84546C2049E810E1
