

17 harmful applications Android users need to delete urgently

ESET, a security company based in Slovakia, has detected an alarming increase in fraudulent loan applications on Android since the beginning of this year.

ESET, a security company based in Slovakia, has detected an alarming increase in fraudulent loan applications on Android since the beginning of this year.

ESET said, in fact, these applications are designed to lend high interest rates combined with spyware that collects victims' personal and financial information for blackmail. Therefore, ESET has identified these applications as SpyLoan - the common name for malicious money lending applications.



These applications claim to be 'legitimate personal loan services' that provide quick and easy access to personal spending funds. This is to trick users into signing up for much higher interest payments than prescribed and shorter loan terms. Bad actors advertise loans through SMS messages and social media.

ESET said the target of these applications is users living in Southeast Asia, Africa and Latin America.

ESET identified 18 SpyLoan apps with millions of downloads and reported them to Google. After receiving the notice, Google removed 17 'SpyLoan' apps from the Play Store.

The list of 17 SpyLoan applications that have been removed by Google from the Play Store includes:

1. AA Kredit
2. Amor Cash

3. GuayabaCash
4. EasyCredit
5. Cashwow
6. CrediBus
7. FlashLoan
8. PrestamosCrédito
9. Prestamos De Crédito-YumiCash
10. Go Credito
11. Instantáneo Prestamo
12. Cartera grande
13. Rapido Credito
14. Finupp Lending
15. 4S Cash
16. TrueNaira
17. EasyCash

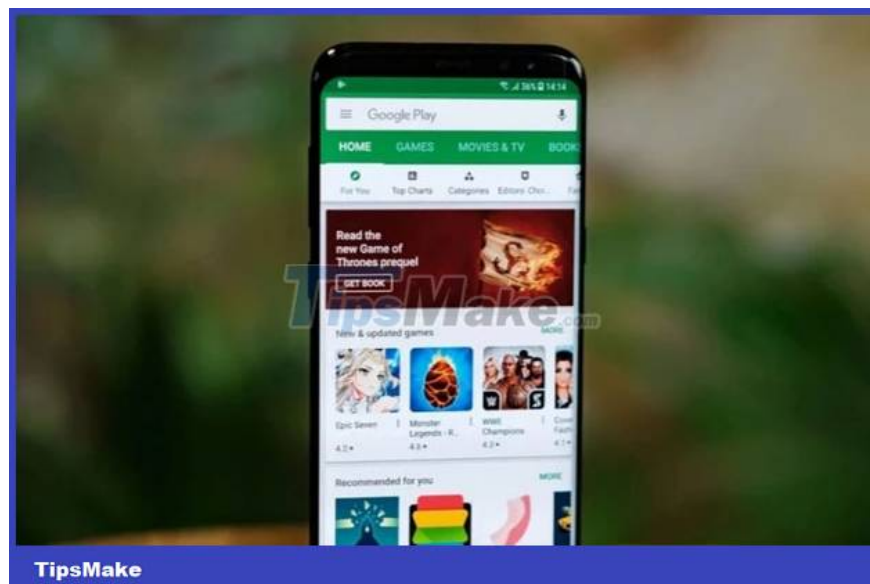
These applications had a total of more than 12 million downloads before being deleted, so if they were accidentally installed, Android users need to uninstall them from their devices.

The only remaining application in the report that was not removed because it has now changed its behavior is no longer the SpyLoan application.

18 malicious applications contain malicious code that displays ads, need to be deleted immediately

Security experts at Dr. Web have just discovered 18 malicious applications impersonating many games and utilities to attract users. These applications that have bypassed Google Play's censorship system contain malicious code that displays ads, thereby generating revenue for hackers.

Before being discovered, these applications had achieved millions of downloads, generating huge revenue for hackers.



Not only displaying ads, some malicious code also has the ability to access various information on the device, putting users' data and privacy at risk.

The detailed list of 18 malicious applications includes:

1. Agent Shooter
2. Rainbow Stretch
3. Rubber Punch 3D
4. Super Skibydi Killer
5. GazEndow Economic
6. MoneyMentor
7. TKF Program
8. FinancialFusion
9. Financial Vault
10. Invest Calculator
11. Eternal Maze
12. Jungle Jewels
13. Stellar Secrets
14. Fire Fruits
15. Cowboy's Frontier
16. Enchanted Elixir
17. Beauty Wallpaper HD
18. Love Emoji Messenger

Recently, a series of malware on the Android platform has been discovered. This shows that malicious applications, using many different tricks, have bypassed Google's censorship system and appeared widely on this app store.

Therefore, according to security experts, smartphone users need to be very careful every time they install applications, even if they are downloaded from Google Play.

In case the above malware has been installed, users need to quickly remove it from their devices.

To remove malicious applications on Android smartphones, you need to access Settings/Settings -> select the Applications tab -> select Manage applications -> find the application to remove, click on it and select Uninstall Install or Uninstall.

Immediately remove these 12 harmful applications from your smartphone

Security experts at Doctor Web have just issued a warning about a series of malware containing many different types of malicious code such as FakeApp, Joker and HiddenAds.

According to Bleeping Computer statistics, these malware have attracted more than 2 million installations on the Google Play app store.



These software will silently run in the background and automatically access ads to generate revenue for crooks, making it very difficult for users to detect. Meanwhile, some other malicious applications direct users to fake websites for the purpose of fraud.

Below is a list of malicious applications discovered by experts at Doctor Web:

1. Super Skibydi Killer
2. Agent Shooter
3. Rainbow Stretch
4. Rubber Punch 3D
5. Eternal Maze
6. Jungle Jewels
7. Stellar Secrets
8. Fire Fruits
9. Cowboy's Frontier
10. Enchanted Elixir
11. Love Emoji Messenger
12. Beauty Wallpaper HD

Security experts reported their findings to Google and now the 12 malicious applications above have been removed from the app store.

According to experts' warnings, if users have installed these software, they should quickly remove them from their devices immediately to avoid being scammed and losing money.

19 harmful applications that experts warn need to be removed urgently

Recently, security experts at Malwarefox discovered 19 malicious applications hiding in the shadow of support utilities that can insert malicious code into users' phones.

These apps are designed to infect users' devices with malicious codes or files. Attack targets are computers, laptops and Android phones. After successful intrusion, malicious code installed in the application will attack

and collect banking information, passwords and user identities.



The most common malware found in these 19 Android apps include Harly, Joker, and Autolycos. In particular, Joker malware has the ability to steal contacts, SMS messages, detailed information about the victim's device and register for paid services without the user's consent.

Harly malware will steal data about the victim's device, especially mobile network data.

Millions of people have downloaded these malicious applications. Therefore, experts warn that users should delete them immediately if they have ever installed them. Below is a list of 19 malicious applications:

1. Vlog Star Video Editor
2. Creative 3D Launcher
3. Wow, Beauty Camera
4. Gif Emoji Keyboard
5. Instant Heart Rate Anytime
6. Delicate Messenger
7. Simple Note Scanner
8. Universal PDF Scanner
9. Private Messenger
10. Premium SMS
11. Blood Pressure Checker
12. Cool Keyboard
13. Paint Art
14. Color Message
15. Fare Gamehub and Box
16. Hope Camera-Picture Record
17. Same Launcher and Live Wallpaper
18. Amazing Wallpaper
19. Cool Emoji Editor and Stickers

To ensure safety, experts recommend that users should only download applications from Google Play for Android and App Store for iOS, avoid downloading strange applications from other sources.

You finished reading the article "**17 harmful applications Android users need to delete urgently**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

