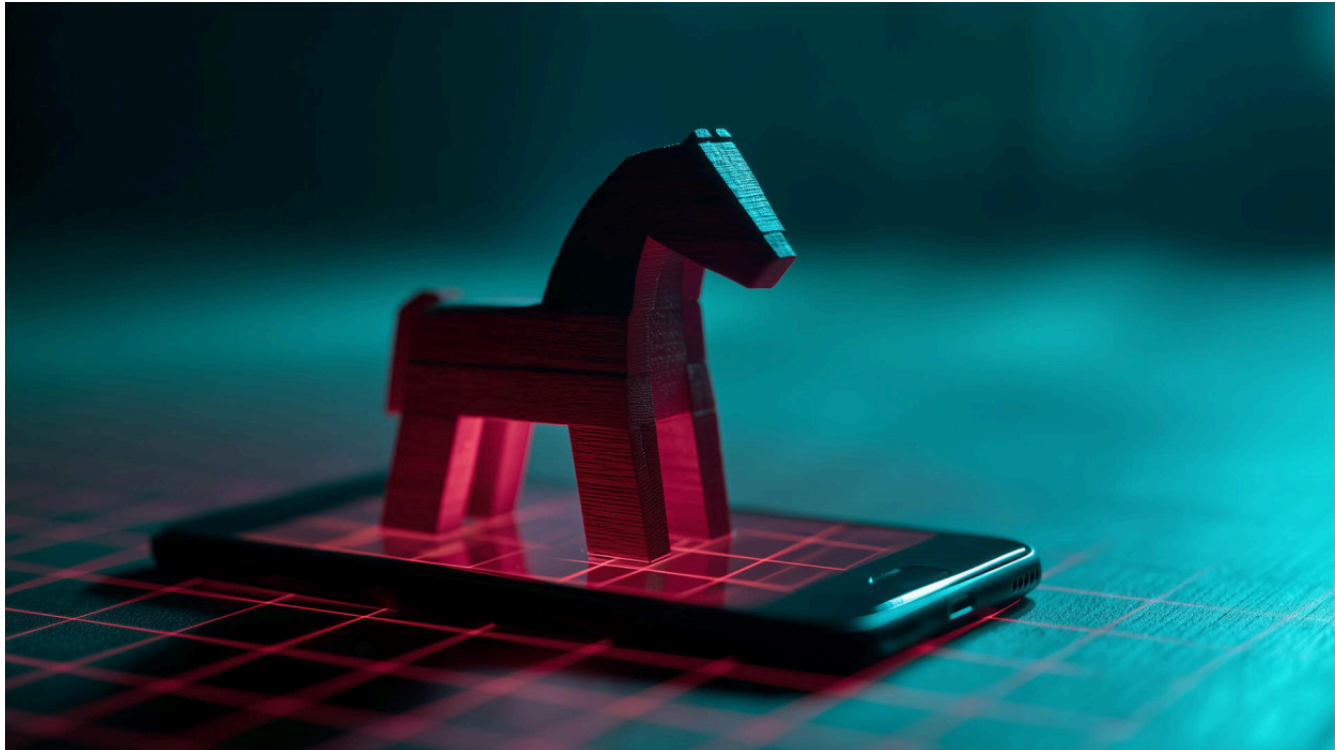


BTMOB: A stealthy RAT burrowing deep into Android devices

 welivesecurity.com/en/malware/btmob-stealthy-rat-burrowing-deep-android-devices



Our recent review of threat detections in Brazil surfaced BTMOB, an Android remote access trojan (RAT) that is less notable for detection volume than for the damage it can wreak. The combination of phishing-led delivery, ready-made app-building tooling and device takeover capabilities makes BTMOB a threat to watch well beyond Brazil or Latin America.

BTMOB at a glance

[First described](#) in February 2025, BTMOB has evolved from the SpySolr malware. Unlike banking trojans, which “only” aim to steal people’s financial credentials or intercept their financial transactions, BTMOB gives adversaries broader options: exfiltrate a range of sensitive data, capture screenshots and record activity on the device, and ultimately take remote control of it. The RAT is also sold with an APK builder interface, allowing anyone to generate new payloads and adapt phishing lures for specific regions at a rapid clip – and without writing any code.

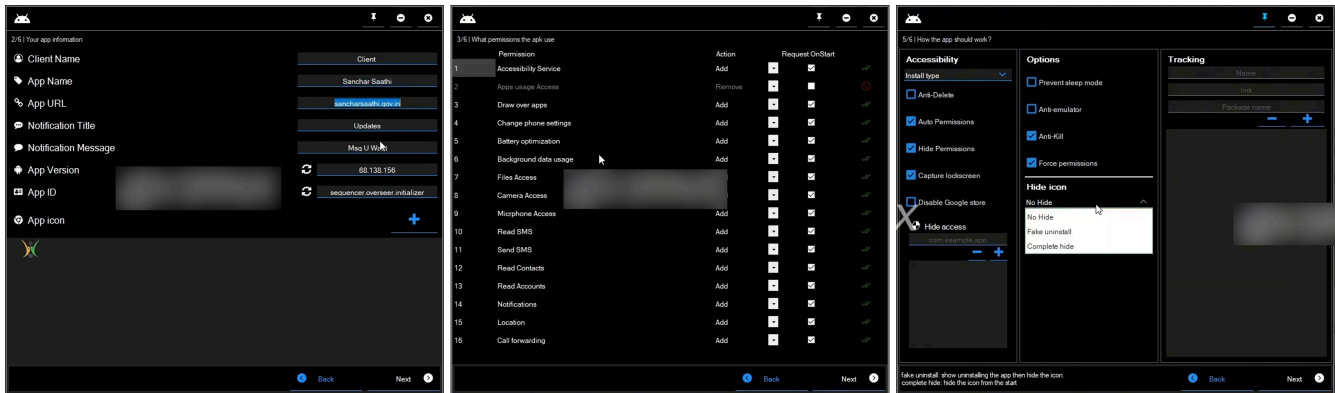


Figure 1. BTMOB APK creation tool

How does BTMOB spread?

Unsurprisingly, everything starts with ordinary social engineering. Operators send victims to phishing websites that pose as streaming services, cryptocurrency mining platforms or other familiar online services. From there, victims are pushed toward fake app stores that mimic legitimate repositories and prompt them to install a malicious APK. Bad actors have also been spotted tailoring their lures to specific regions.

Once installed, BTMOB seeks extensive access to the device. As is common these days, it abuses Android Accessibility Services to gain elevated permissions and grant itself further system access without additional user interaction.

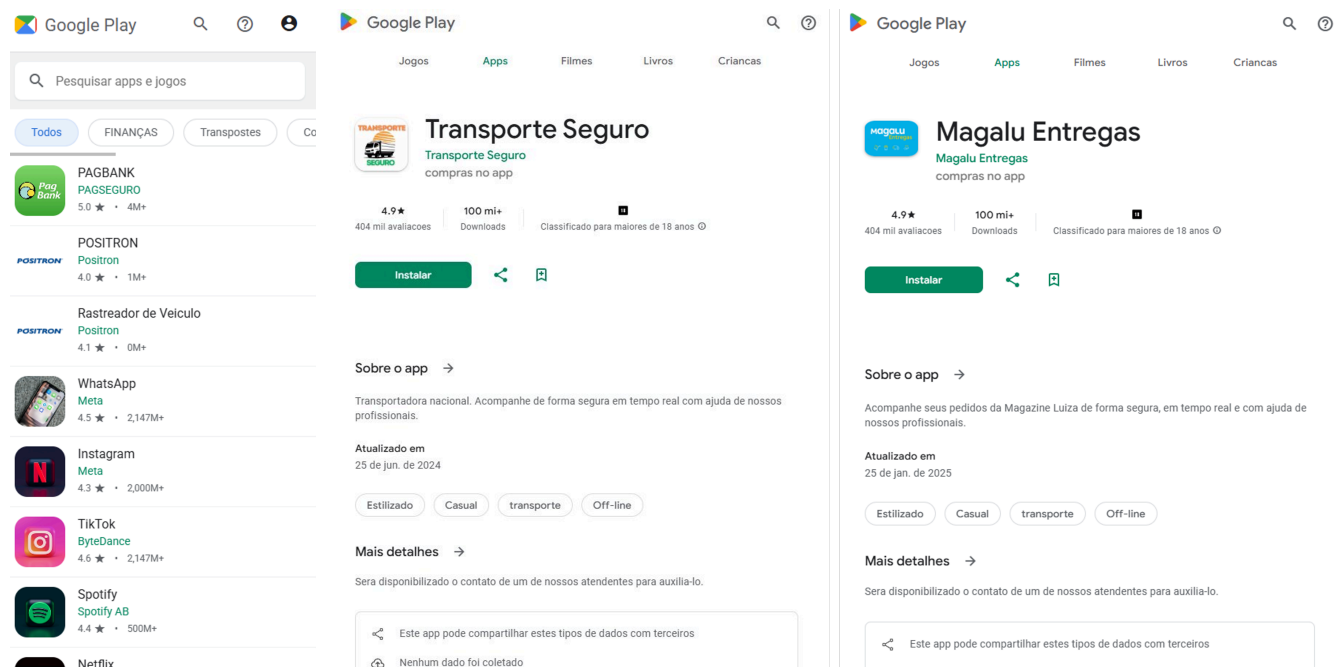


Figure 2. Fake app store and malicious apps. Source: [@Merlax_](#)

Since it's built for the malware-as-a-service (MaaS) economy, BTMOB is marketed as a software product, including through a promotional page on the open web that funnels

prospective buyers to a Telegram operator. The sales pipeline extends across social media platforms, with a number of accounts on X and Instagram actively peddling the tool.

BTMOB RAT

BT MOB • btmob rat • bt-mob rat

\$700 / month

Most powerful Android RAT 2025 – 100% undetectable

Buy for \$700/month

Contact @craxso

BT MOB

Broadcast

Redirect

Updates

8075

Search clients

Spoofer

United Kingdom

01 198 80 38

Android 14

N/A

2023-11-22

v3.4.1

50%

N/A

Please share 14

My source

388 ms

Power

14.1

Figure 3. BTMOB offer on the surface web

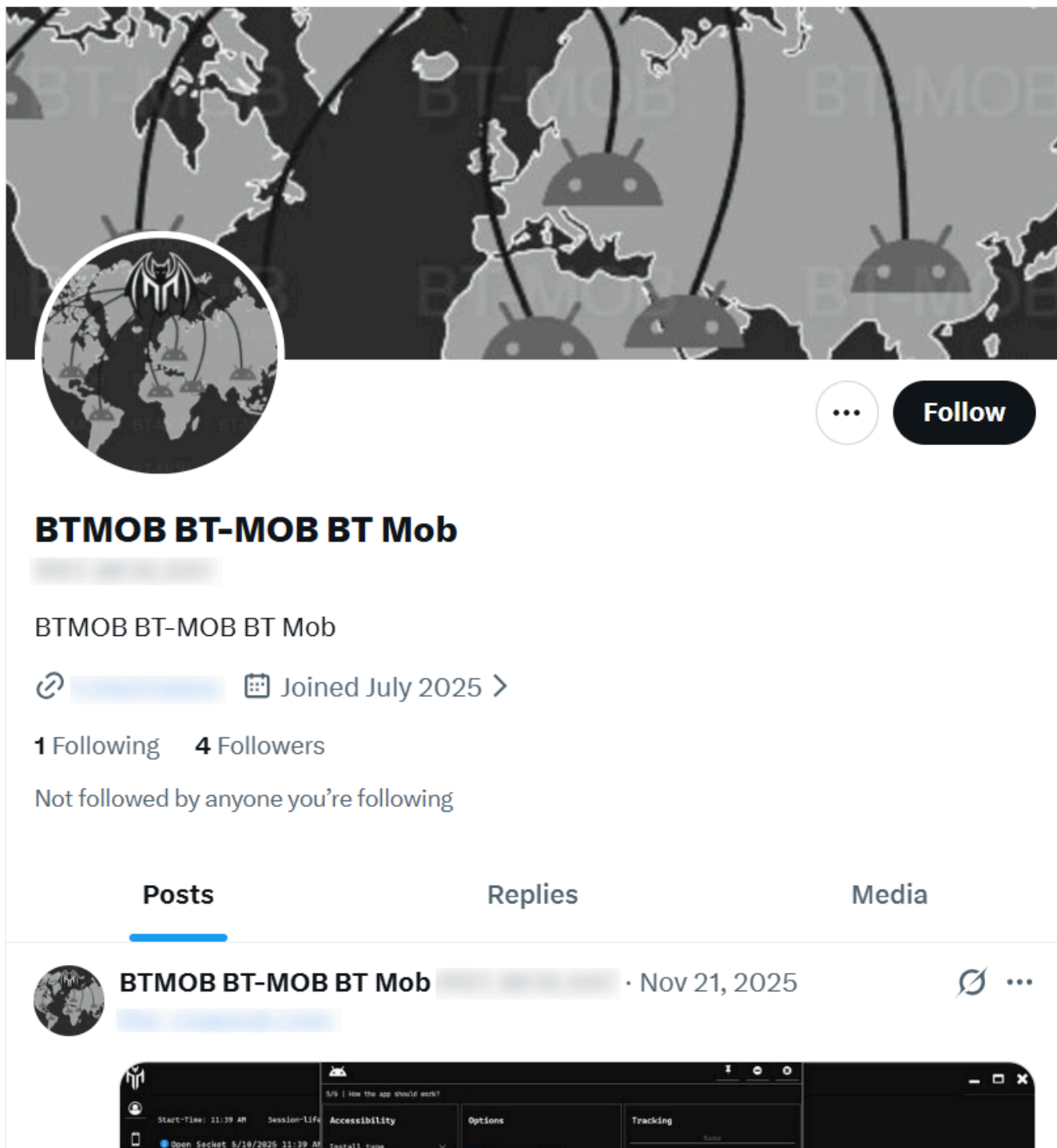


Figure 4. X profile linked to the malware

Once someone purchases the malicious kit, they can adapt its features, including the phishing lures so they impersonate the brand or agency most likely to lure victims in any given country. For example, researchers [Johnk3r](#) and [Merl](#) recently spotted campaigns that spread BTMOB while impersonating Argentina's tax and customs authorities.

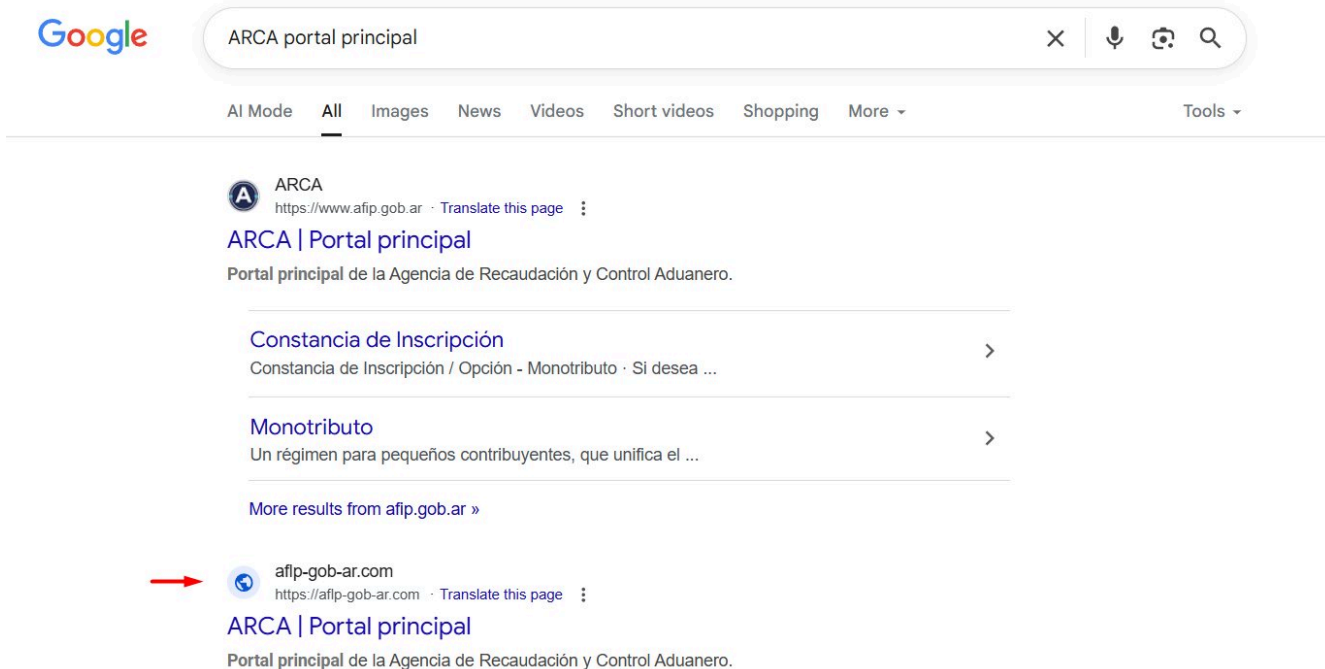


Figure 5. BTMOB impersonating an Argentine government agency. (Source: [Germán Fernández Bacian](#))

Market dynamics and detection challenges

Even where developers initially restrict the tool to paying customers, the economics remain favorable for attackers. A reported \$5,000 lifetime license plus a monthly support fee is low compared with the returns a successful fraud operation can generate.

In addition, the MaaS model also lowers the barrier for less sophisticated adversaries. In January 2026, a dark web forum claimed to offer BTMOB-related files for free download. The forum later went offline, and our search didn't recover the payload(s), but the episode points to a familiar risk with commercial malware: access rarely stays contained forever and the tool can move into secondary markets through resale, barter or sharing inside closed groups. Competing malware families can also copy some elements that make payload customization and campaign management easier for less skilled criminals.

As new variants can be generated quickly, defenders should expect rapid payload turnover rather than a stable set of threats. ESET products detect the primary tool as MSIL/BtmobRat, while related Android variants trigger detections such as Android/Spy.Agent.EED, Android/Spy.Agent.EIJ and Android/Spy.Agent.EIK. [Cyble's report](#) from February 2025 noted that roughly 15 samples of BTMOB v2.5 had been spotted since late January of that year, i.e., in a mere two or so weeks.

How to protect yourself

A few basic tips will go a long way toward staying safe from BTMOB and other Android malware:

- Stick to the official app store: Attackers rely on fake app stores that mimic Google Play. Organizations should mandate that users download software exclusively from official repositories.
- Treat links with suspicion: Be skeptical of unsolicited links delivered via email, messaging apps, social media, and targeted advertisements.
- Use security software: Both individuals and organizations should use mobile security solutions and treat mobile devices with the same rigor as other machines and environments. Corporate security teams must make it clear to employees that a single rogue download could expose the company's crown jewels.

Indicators of compromise

Because BTMOB 'mutates' quickly, many indicators may age rapidly. Nevertheless, specific infrastructure patterns often recur across different samples and aid in triage.

IP addresses

74.125.202.103	142.251.183.138	173.194.193.138	173.194.206.106
178.156.177.192	191.101.131.250	195.160.221.203	104.21.64.137
173.194.194.94	191.96.224.87	191.96.225.241	191.96.78.172
191.96.78.28	191.96.79.133	191.96.79.179	191.96.79.41
192.178.209.95	200.9.155.153	74.125.132.95	78.135.93.123
79.133.57.141	arbsniper.com		

Hashes - SHA256

Hash Value

58AC130A8EBB09E37592AC69841483EDC5695D1545B1F04F23D5B760AC17CD94

0A542751724A432A8448324613E0CE10393E41739A1800CBB7D5A2C648FCDC35

Hash Value

A764D73795ABE47AE640BA09999A18C47B5340E5ECC7B897AFEBF34F3F37638F
26A2268281E8043125EF72B92F8980B42912048753D56894BC378FB54C7C188A
6AE94CE710016D86ED7457236DEEF2C4C51478587F3609B6E827A348828B3931
E5A9FDFF900DD502E8F3DCE52D2D1B69AA9AFAFB5094A28F9037E8770DB0E63B
C6199E175FB988CBBEACDF0F5ACDF9ED83F5BDAAE5C95B7A6C27EE72CD11B0B1
6BBA64FA9E8A7B11CB2476CD071DE08986DB44B0783EFF211C68FA5594EF8143
5AAAF972C8BF39A98F2748E526DE3CC0370BA831997D7D9765CDABA599645C0D
5AAAF972C8BF39A98F2748E526DE3CC0370BA831997D7D9765CDABA599645C0D
DDCE0219923D152B8FACD303F058A6286CF1F6924992B9FB9F5BF4D96436CC39
D55057CD9110D12A192281356F06B94F342B9FEBB305CF0A5898A7E6AF40758F
676CB2D0A60403AFC06CEA1B572CB7261F706365FAC65621B5A4907893E7AC0D
75DD4FB011ED598374A46FC0D9C0D1D64A298341C34AFC83A56A6983CFD27764
702261BA38B57ECC3A5407FED28B2F0611A74C2EC0C116AEA4F9E6DEF0899AED
998A7ED1572AD9DC11375BC25294E1954E606B7CFF9FABC5C120713E597CD274
244D81FD9908CD17815501D4EDADEB1BAF1C421AA25D8BD61C7CB481C939540E
512EDE9F2FA794907999F3C26165557FDFD383B7AAD71BA022CE2C8BA6C0019D
7AC974899E8E05AAACD417577C97E382D5E8C5F7F4A85632CFFB47EC2F6AE4E0
168F50BF9A87099094EF410E3AC33E676A6A8740A5437CD09E7B63D73DF8431A
2525D1E427A9983B0B4CA0906A4B44FFB9814B23D53FD8A2E3AB6512B027C733
6101D1E1811DB052F869F7EB3402DAD28DA7E92103D4A44EE43F95846A075012
1A60CB5F7E2FB7C09FC3DC8459108B26AC98EE73131F37A28CFDAD5FC75B7A7D
97A0497DE585D3BE6EC75064AB3BD0979CD85561193C1F0669CCF4DB31330687

Hash Value

02A52C4CC11748D44C9B49D508EE4E46425661981FA1406F30EC0830CB69DDC5

6F9832EBB4C3054BEE4A6CE5CCB69C00E2020053E1308353343097E6A4041109

F76B13040C634F82A8332FF9443D84C89A5BCED51AE9ADAD7FD15C05FADB4324

C99139B0053C4C698EA0246D26D747F2A984C7ABA4613DA818ECD9F97899EF3A

8F09274E808E0063D51F34CAC82A5770B3DF30C792E426DA2F6A80657F27AFFC

140A7F995B0336942691A2E93E2017FD575267C017C7D0728D69169306F91963

A1E457C52EAB430C20D48F2AC476E080386313F16EFB135A0471902CF68CE475

5A4E86BBCF0EBC455D2995DB225D9AD682E9B37B6BAD472A604A462099D988BD

A892F1EF2E530D67BF948A48C734DA3F27718EB8B883CA0B686DDB0A81071731

AA56F350882CE63429C6626567487B041F06168BB60F4FC371A262EABADFA660

752C1CFE783ED343E470AB95A4843A23872CDC98B7D3ED5633DD6C881C071A14

0628AD6D1FD836B13B22E75FA169502D8CE78B7AD20F0261EB5151DA98437BCA

6844CE1539014571360495C6FB50965E813C2721663BDD40D577D9E5163773C6

ESET detection names

Detection name

Android/Agent.FQK

Android/TrojanDropper.Agent.NES

Android/Spy.Agent.EIJ

Android/Spy.Agent.EIK

Android/TrojanDropper.Agent.NDK

Android/Spy.Spysolr.A

Detection name

Android/Spy.Agent.EUG

Android/Spy.Agent.EWN

Android/Spy.Agent.FFE

Android/Spy.Agent.FFL

Android/Spy.Agent.ELM

Android/Spy.Agent.FFM

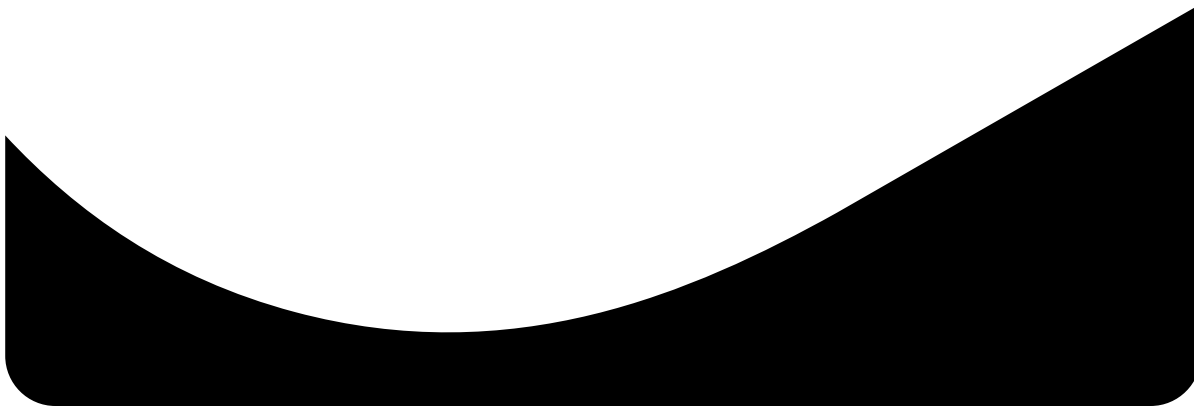
Android/Spy.Agent.FEE

Android/TrojanDropper.Agent.NBO

Let us keep you up to date

Sign up for our newsletters

Ukraine Crisis newsletter Regular weekly newsletter



Related Articles

[Malware](#)

[SnakeStealer: How it preys on personal data – and how you can protect yourself](#)

[Malware](#)

[Beware of threats lurking in booby-trapped PDF files](#)

[Malware](#)

[Watch out for SVG files booby-trapped with malware](#)