Crocodilus in the wild: Mapping the campaign in Poland

medium.com/@mvaks/crocodilus-in-the-wild-mapping-the-campaign-in-poland-15d3078eb954

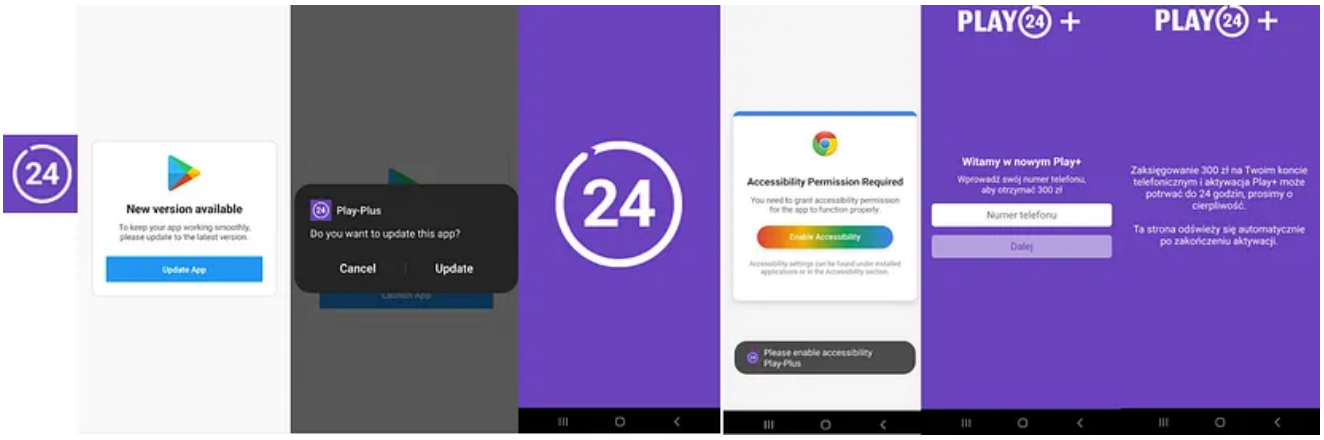
May 30, 2025

--

Over the past week, several malware distribution campaigns have been observed in Poland, all targeting Android users with the same goal — full control over the device and theft of credentials.
Each campaign impersonated a well-known Polish brand — including a major bank, e-commerce platform and telecom provider — using fake apps to trick victims into installing malicious software.
Despite the use of different themes and brands, all three campaigns relied on malware from the Crocodilus family. Shared infrastructure — including the same AES key for traffic decryption and a common C2 address — strongly suggests they were orchestrated by the same Turkish-speaking threat actor.

Play-Plus campaign

A campaign impersonating the telecom provider **Play** used an app with an icon very similar to the legitimate one.
Upon launch, the app displayed a message prompting the user to update the Play Store, which in reality was a request to allow the installation of additional applications by the malware.
The dropped application then requested access to Accessibility Services in order to take control of the device.
The user was asked to enter their phone number to supposedly receive 300 PLN on their mobile. They were told the bonus would be activated within 24 hours, likely to delay suspicion and allow the attackers time to act.



IOCs

Dropper:

```
package: collie.armchair.puppet MD5: 47687323c7a37ee5ab1c34226b23a360dex file:
submersedfeast.dexinstalls: rVwMwHK.apk
```

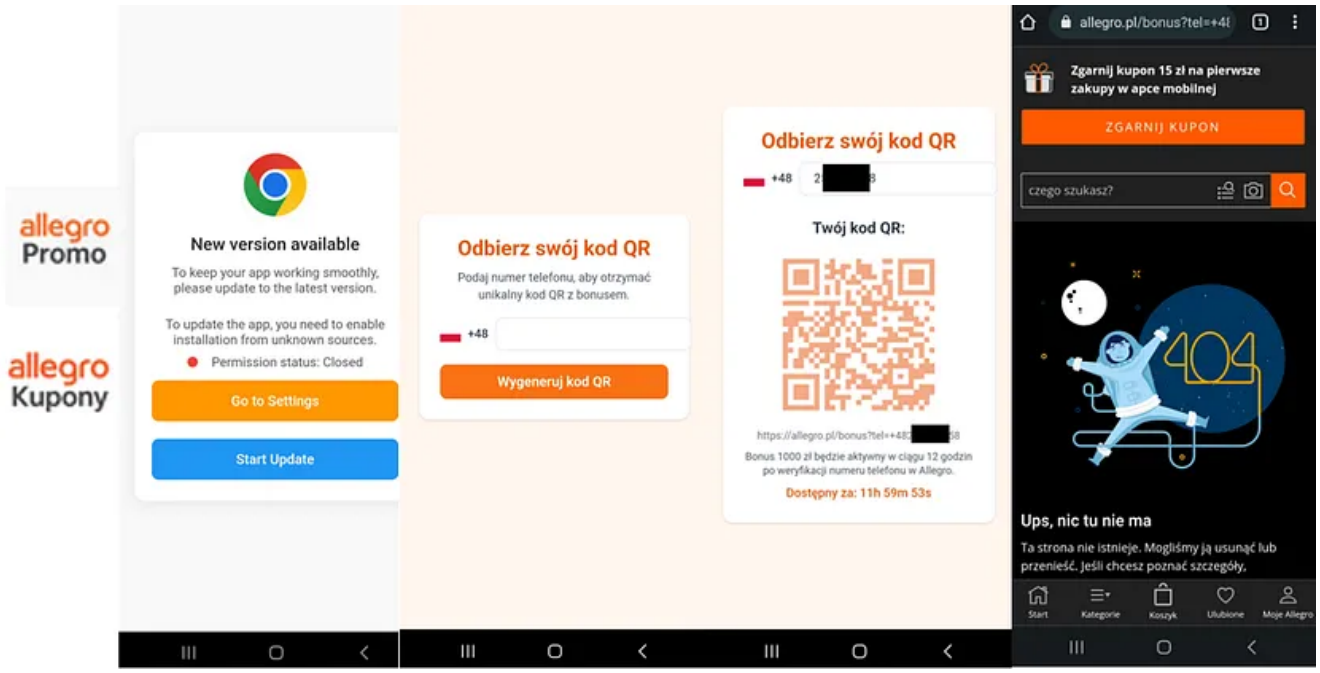
Extracted .apk:

```
package: untitled.lividly.disobeyMD5: dc966268be1c40447c73bfc01808dd83dex file:
hermitcrudely.dexC2: 7162abdd9fd6e28.clickAES Key: DBeYRNqiFnsyGpY8
```

Allegro campaign

A campaign impersonating **Allegro** was distributed via the following URL:

```
hxxps://allegro-kupony.sbs/Allegro%20Promo_3.16.apk
```



The downloaded app, named *allegro Promo*, displayed a message upon launch prompting the user to allegedly update their Chrome browser. It then installed another application embedded within its resources.
The dropped app — *allegro Kupony* — asked the user to provide their phone number and subsequently generated a QR code, supposedly granting a bonus of 1000 PLN.
The link included in the app followed this format

```
hxxps://allegro.pl/bonus?tel=+48(phone number)
```

directing the victim to a non-existent resource on Allegro's legitimate domain.
The attackers added a message stating that the bonus would be activated within 12 hours — likely to avoid raising suspicion and buy time for further malicious activity.

IOCs

Dropper:

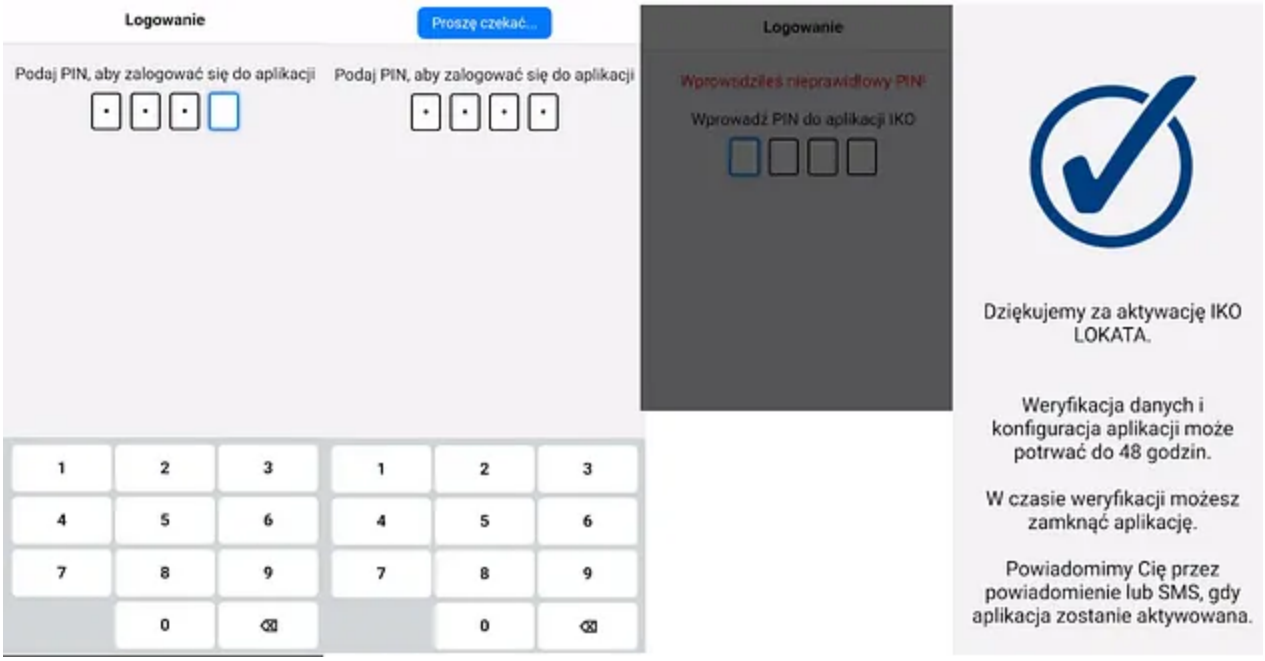
```
package: alfalfa.ungodlyMD5: aca6cc169fe860fe9230d99206a98d12dex file:
lapelrover.dexinstalls: xdjoN.apk
```

Extracted .apk:

```
package: shore.footprintMD5: dc966268be1c40447c73bfc01808dd83dex file:
confettiunkind.dexC2: rentvillcr.homesAES Key: DBeYRNqiFnsyGpY8
```

IKO campaign

The campaign described in my previous analysis was distributed through fake social media ads promoting the opportunity to receive allegedly attractive interest rates on bank deposits via a new application.
The app leveraged Accessibility settings to gain control over the device.



IOCs

Dropper:

```
package: purge.trembleMD5: 689579531a417b84ddbceb17c75d3c39dex file:
ablemocker.dexinstalls: iSZMv.apk
```

Extracted .apk:

```
package: unrelated.hamburgerMD5: e7551da0d6e05cce11d4bf3ae016bb15dex file:
jasminenacho.dexC2: rentvillcr.homesAES Key: DBeYRNqiFnsyGpY8
```

Additional .apk found on VT:

```
package: nuttiness.pamperer.cosmeticsMD5: f6f589d1a0a189aded4d008b671be0dbdex file:
gullyclosure.dexC2: rentvillcr.homesAES Key: DBeYRNqiFnsyGpY8
```

Thanks for checking out my analysis — I'll update the article if any new campaigns pop up :-)