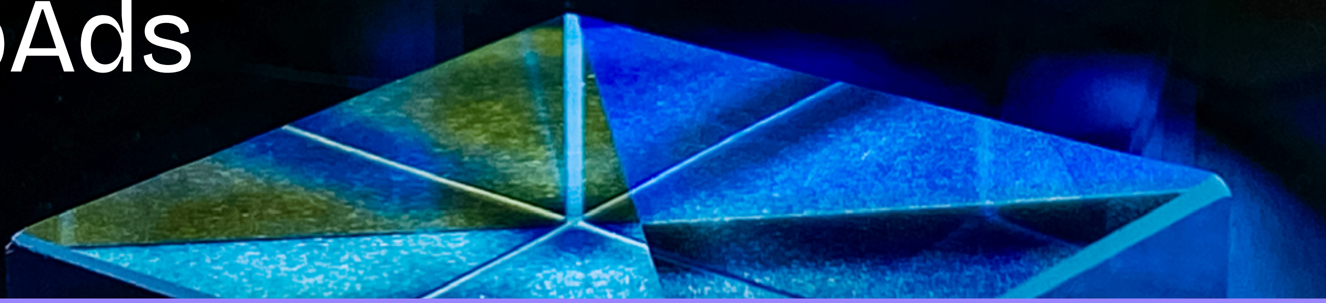
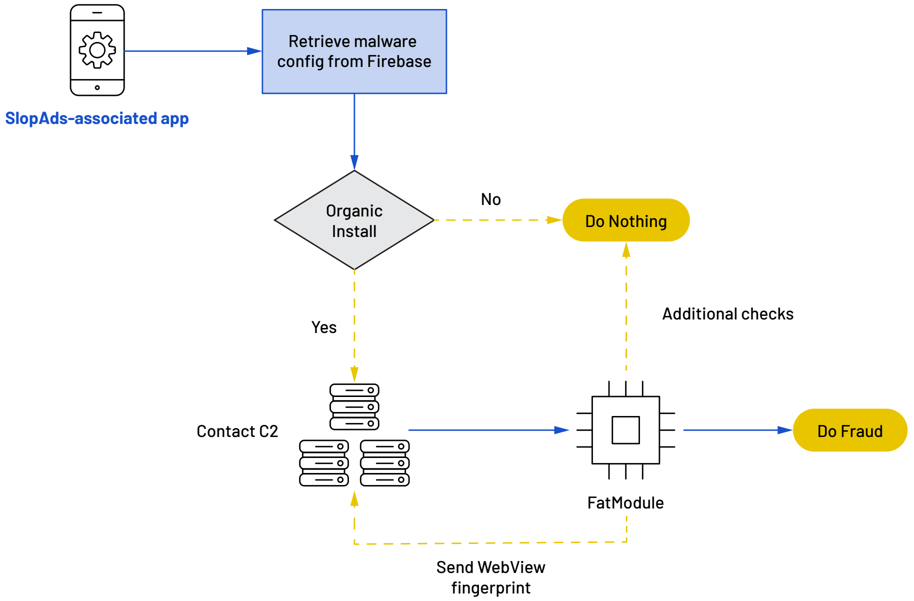
HUMAN | SATORI

Satori Research Bulletin: SlopAds



Sophisticated ad and click fraud scheme hides malicious code in image files

How SlopAds Worked:



1. Check if SlopAds app was downloaded from the threat actor's ad campaign.
2. Contact the C2 server, download **FatModule**, and send device/browser info to threat actors.
3. Perform final checks to avoid detection.
4. Begin ad and click fraud.

Key Findings:

- **224** SlopAds-associated apps, and rising
- More than **38 million downloads** of SlopAds-associated apps
- Bid requests in **228** countries and territories
- **2.3 billion bid requests a day** at peak

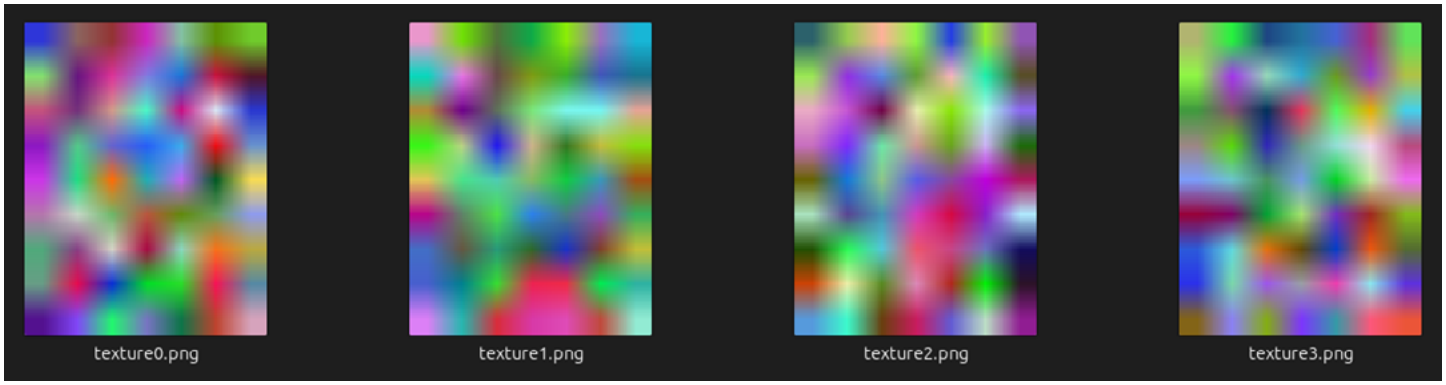
What Makes SlopAds Unique:

Abusing Attribution Tools

SlopAds uses mobile marketing attribution tools to determine if a download was the result of the threat actors' own ad campaign. The apps only attempt ad and click fraud if the app was downloaded because of the ad campaign.

Hiding Code in Image Files

The image files seen below aren't *just* image files, they're also puzzle pieces for **FatModule**, the part of SlopAds that attempts the fraud. Hiding the malicious code in these images is called *steganography*.



Read the full technical report on SlopAds for more details.

Satori researchers discover, analyze, and disrupt threats throughout the digital landscape resulting in actionable insights and collaborative takedowns of cybercrime. Their work empowers everyone in the HUMAN ecosystem, delivering comprehensive insights throughout the customer journey, and benefits that strengthen our unified HUMAN Defense Platform.

About HUMAN

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We enable trusted interactions and transactions across the full spectrum of online actors: humans, bots and AI agents. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information please visit www.humansecurity.com.