

Unboxing BADBOX 2.0

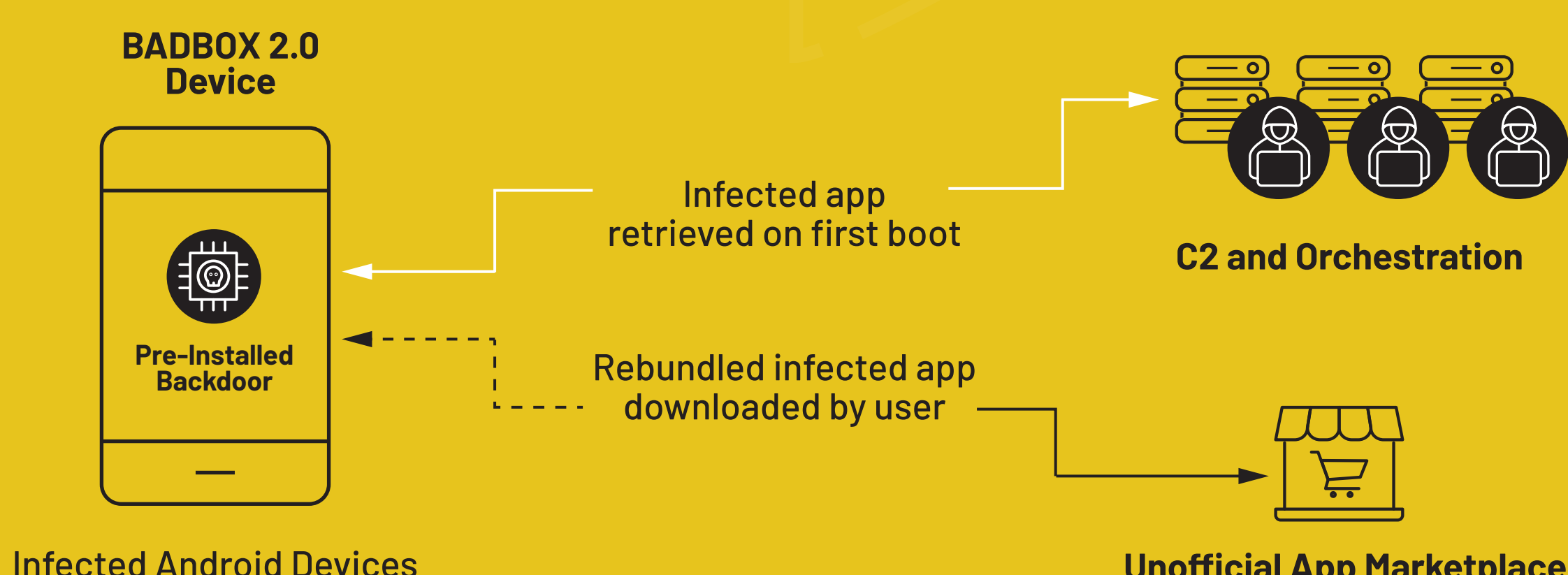
The Satori Threat Intelligence and Research Team's October 2023 report into the BADBOX operation wasn't the end of the story.

In fact, it was just the beginning:



Following the Satori report, the threat actors adapted their tactics, shifted their targets, and started up **BADBOX 2.0**.

BADBOX 2.0 infected **more than a million consumer devices**, including phones, tablets, connected TV boxes, digital projectors, and some aftermarket car infotainment centers.



These consumer devices come pre-installed with the **BADBOX 2.0** malware, download the malware when first turned on, or are infected when an unsuspecting consumer downloads an app from an unofficial app store.




Ad Fraud
Hidden Ads

Apps on infected devices request and render ads where a user can't see them, and report that the ads are coming from separate, uninfected versions of the apps.

HUMAN observed a peak of **5 BILLION** ad requests a week connected to this threat.



Ad Fraud
Hidden WebViews

Infected devices load hidden WebViews which then visit a series of ad-heavy gaming websites so the owner of those gaming websites can cash out.

HUMAN identified nearly **1 THOUSAND** of these cashout gaming websites.



Residential Proxy Creation

The backdoor gives threat actors the ability to sell access to infected devices' IP addresses, facilitating downstream attacks by other threat actors, including account takeover, fake account creation, DDoS, and malware distribution.

Researchers believe the proxy network is responsible for **petabytes** of threat actor activity daily.



Click Fraud

BADBOX 2.0 command-and-control servers directed infected devices to visit one of a collection of low-quality domains and to click on ads there, helping the owners of those sites cash out.




Researchers observed **BADBOX 2.0**-infected devices cycling through a "playlist" of low-quality domains.



BADBOX 2.0 has been **partially disrupted** through the collaborative efforts of **HUMAN**, Google, Trend Micro, Shadowserver, and other partners.

HUMAN customers are protected from the ad fraud schemes in **BADBOX 2.0**, the click fraud scheme where applicable, and bot attacks facilitated by residential proxy.

How to avoid getting BADBOXed:

-  If purchasing an Android device, choose only those that are Google Play Protect-certified.
-  Download apps only from official app marketplaces.
-  Avoid off-brand devices like those targeted by BADBOX and BADBOX 2.0.

To learn more about **BADBOX 2.0**, read our [technical report](#).