



Satori Investigation: BADBOX 2.0

HUMAN Security

- Gavin Reid - Ciso Human Security



BADBOX 2.0 is the name of a complex and sprawling fraud operation centered on a collection of **Android applications and devices backdoored** by threat actors of Chinese origin

The threat actors use these backdoors to perpetuate several forms of fraud, including **programmatic ad fraud, click fraud, proxyjacking**, and **creating and operating a botnet** with the devices

HUMAN uncovered the campaign
through leads gained from observing
adaptations and updates from the
threat actors behind
BADBOX/PEACHPIT

HUMAN is **protecting customers**
from the **ad fraud and attacks**
perpetrated via the residential
proxy network IPs associated with
BADBOX 2.0.

BADBOX 2.0

By The Numbers

**More than 1 Million
BADBOX 2.0–infected devices**
— a substantial increase from
74K BADBOX devices

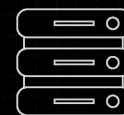
More than 1 Million BADBOX 2.0-infected Devices



Over 200 backdoored applications spread through multiple techniques



Operating bots in **multiple countries**



Orchestrated by **dozens of C2 servers**

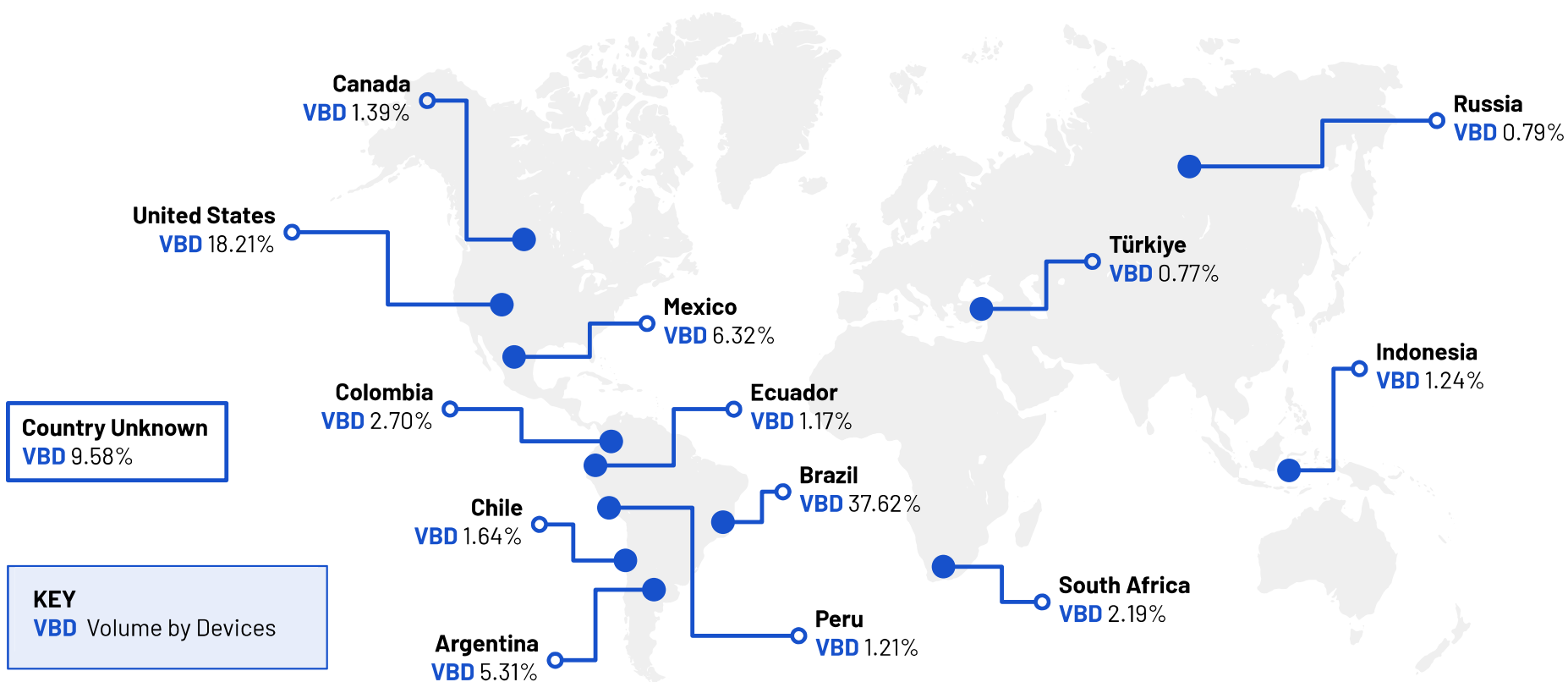


SATORI INVESTIGATION

| **BADBOX 2.0**

BADBOX 2.0 Global Breakdown

BADBOX 2.0-infected devices appeared in 222 countries and territories



Country Unknown
VBD 9.58%

KEY
VBD Volume by Devices



Who's Who in the BADBOX 2.0 Crew

SalesTracker Group: group of threat actors responsible for the original BADBOX campaign. Named after "saletracker" string in network data.

MoYu Group: operator of the backdoors found pre-installed on BADBOX 2.0 devices and bundled into the 200+ apps shared through unofficial app marketplaces. Named after IpMoYu proxy service they sell.

Lemon Group: China-based threat actor group involved in BADBOX, selling residential proxy services. Heavily connected to a multifaceted ad fraud scheme based on a series of HTML5 (H5) game websites

LongTV: part of Longvision Media, a Malaysia-based internet and media company, developers of apps both for its own branded devices and for non-LongTV-branded devices. Enables hidden webview ad fraud.



BADBOX 2.0

Backdoored Devices

Backdoor was **present only on Android Open Source Project-based devices**, specifically:

- TV boxes
- Lower-end/"off brand" tablets, phones
- Projectors
- Aftermarket car head units



Sample of Affected Android Devices



X96 Mini TV Box



X96 Mini TV Stick



X96Q TV Box



X98K TV Box



Transpeed TV Box



TV98 TV Box



TV98 TV Stick



Q8 TV Stick



Sample of Affected Android Devices



H20 TV Box



Tablet



Tablet



Android Car System



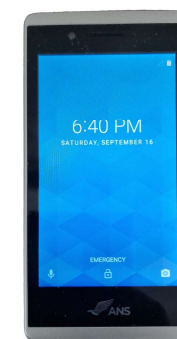
ShockVolt SV55 Phone



Generic Android Phone



Generic Android Phone

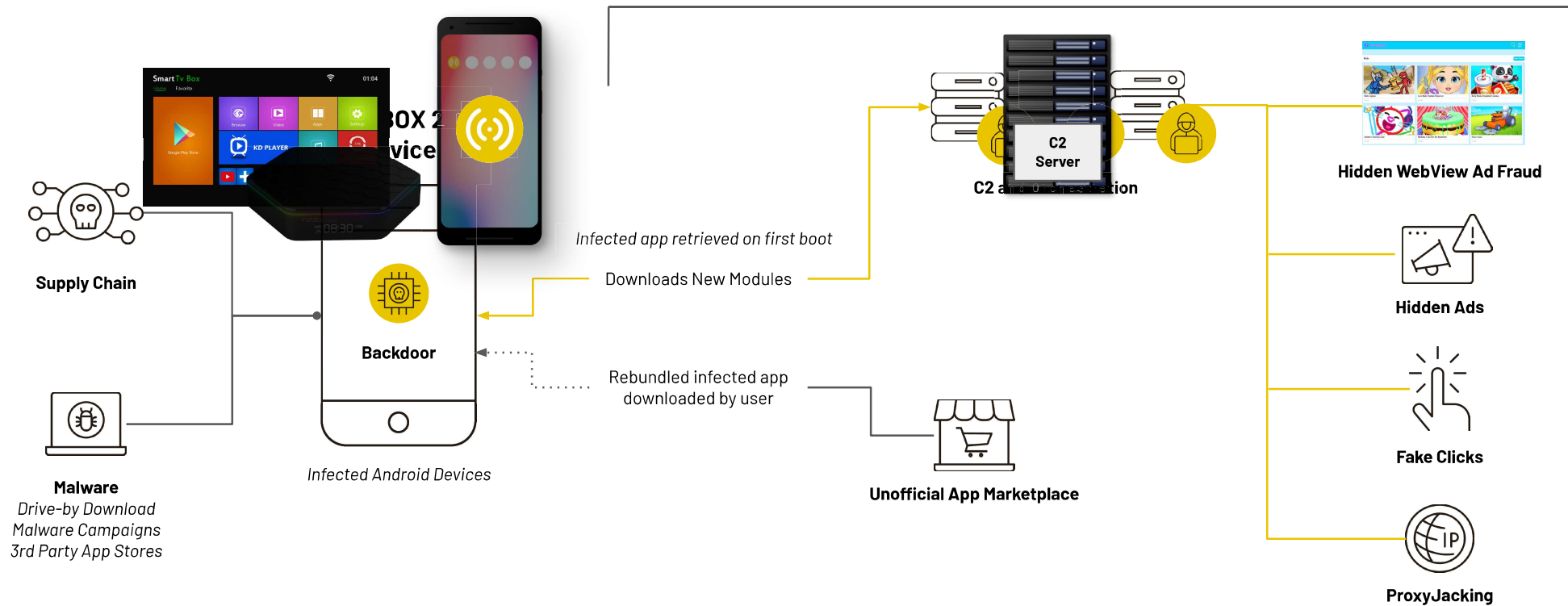


ANS L50 Phone



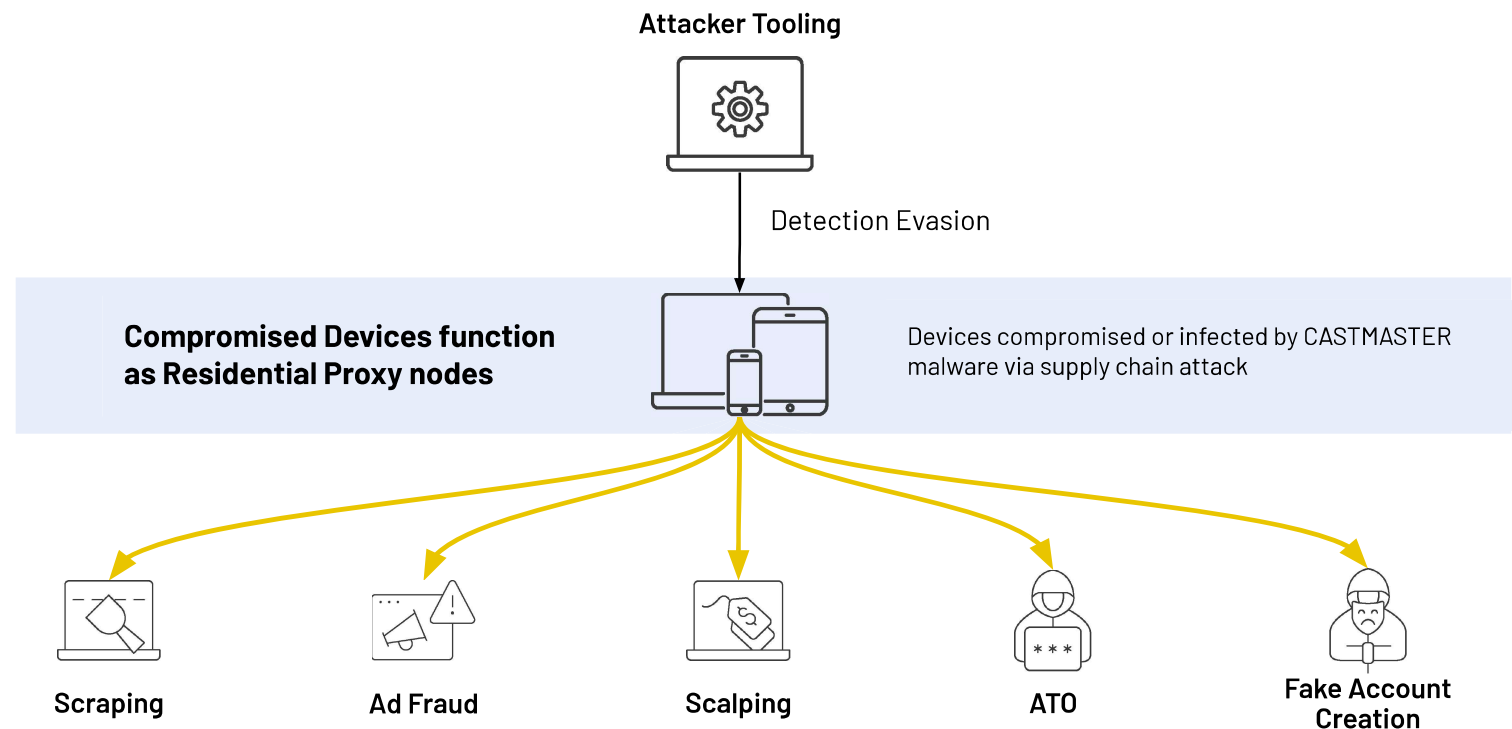
Overview

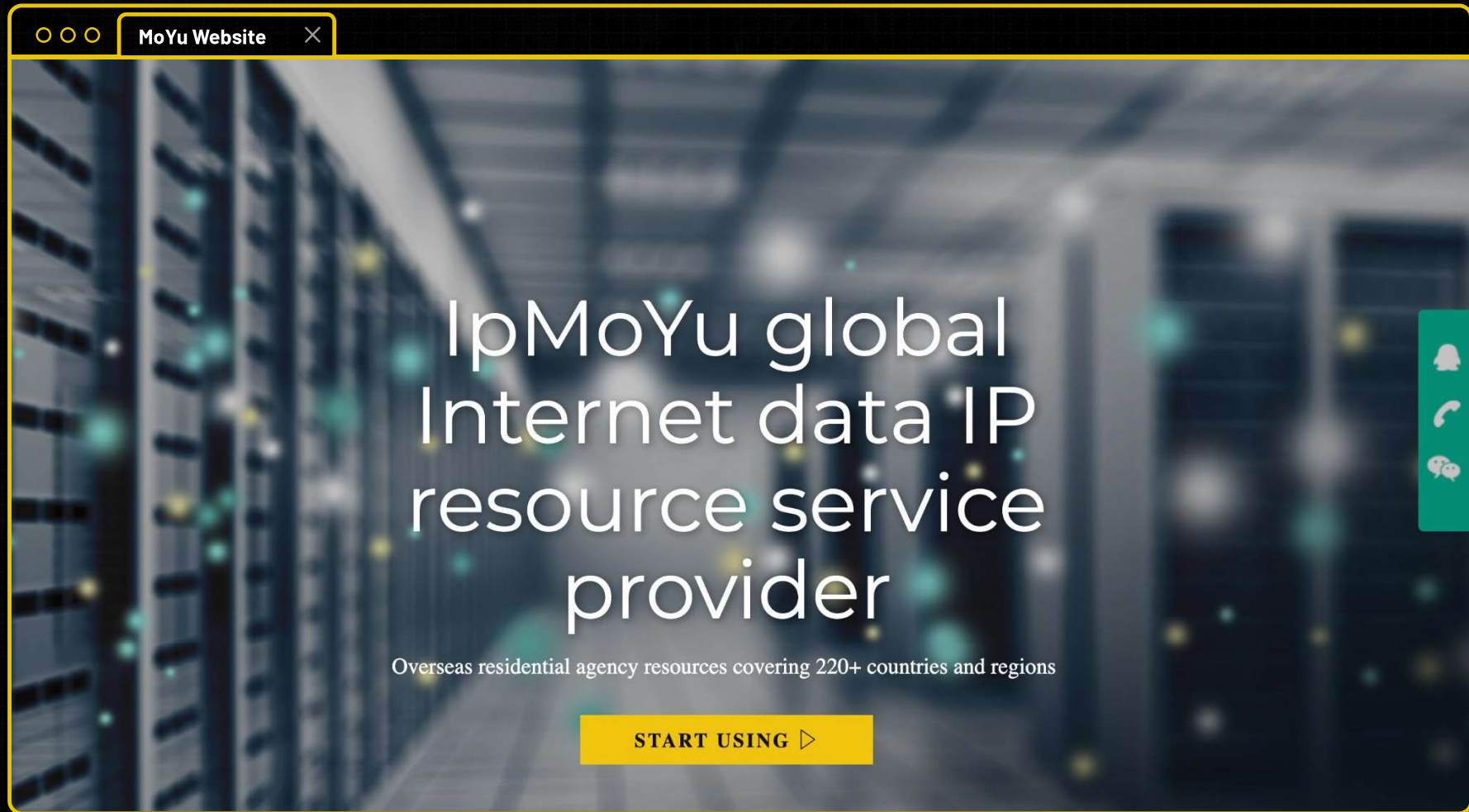
 SALESTRACKER/MOYU



Enterprise: Residential Proxy Network

Similar to BADBOX, HUMAN observed a proxyjacking module that adds devices as a node in a proxy network to which the threat actor sells access to other threat actors





HUMAN identified
2 related ad fraud campaigns
associated with BADBOX 2.0

Smart Tv Box



01:04

Home

Favorite

Hidden ads

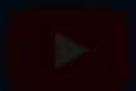
via LongTV launcher apps and
“evil twin” apps



Google Play Store



LONGTV



Music

Clean Memory

**5 billion fraudulent
bid requests per week**

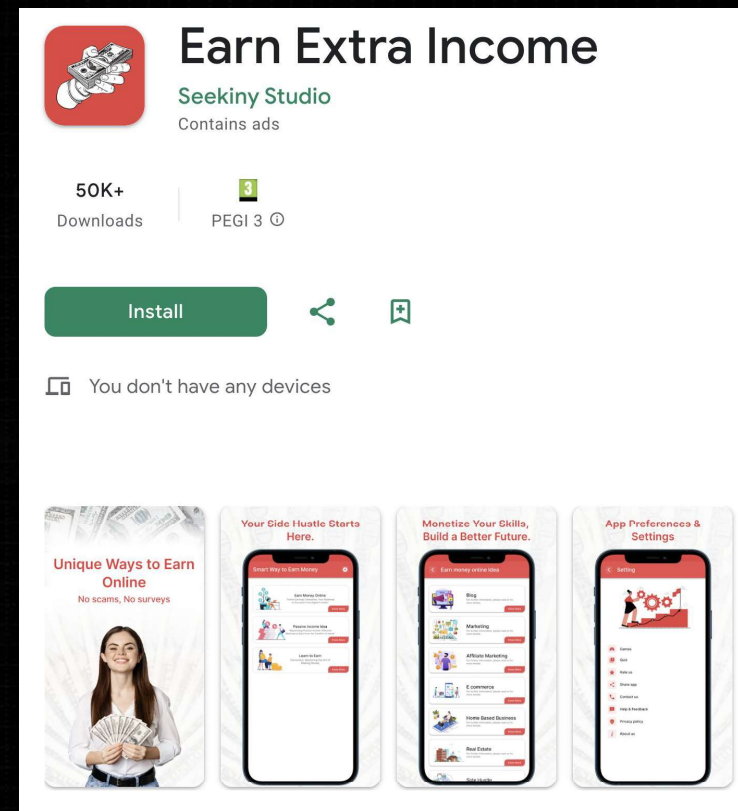
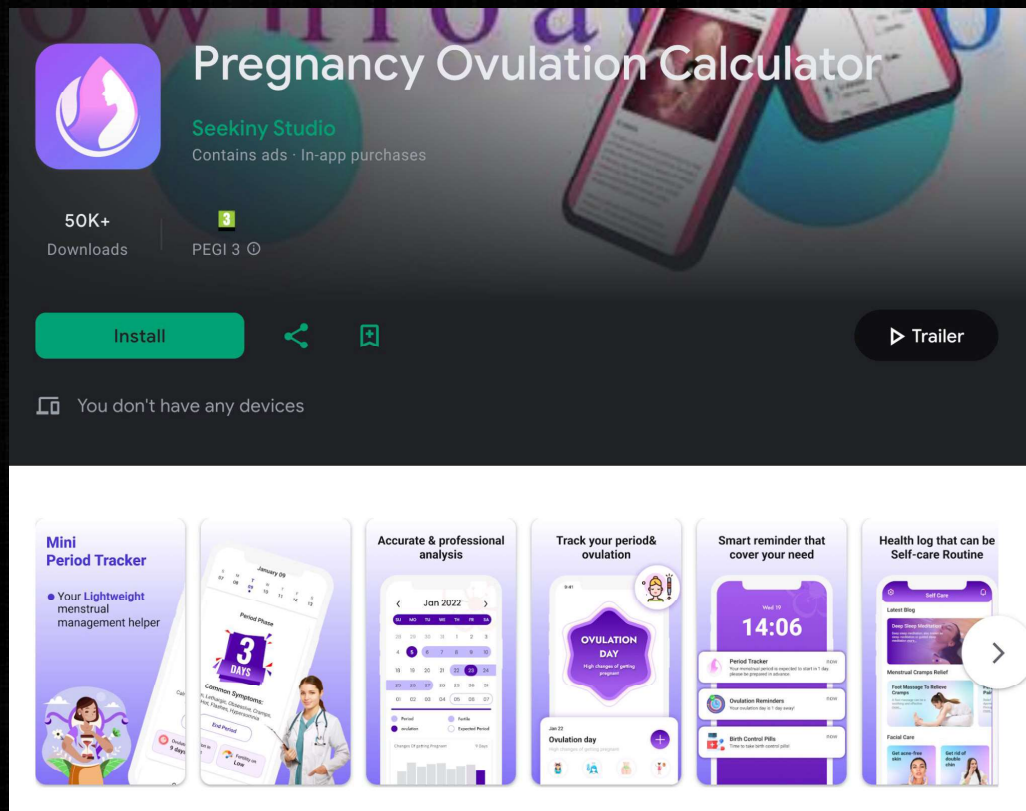


SATORI INVESTIGATION

| **BADBOX 2.0**

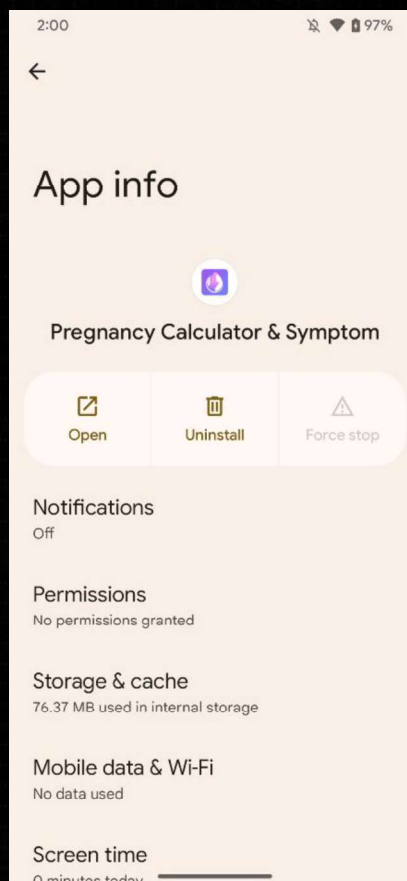
We identified
24 “evil twin” apps
with corresponding “decoy twins”
hosted in the Google Play Store

Example “Decoy Twin” Apps in Google Play Store

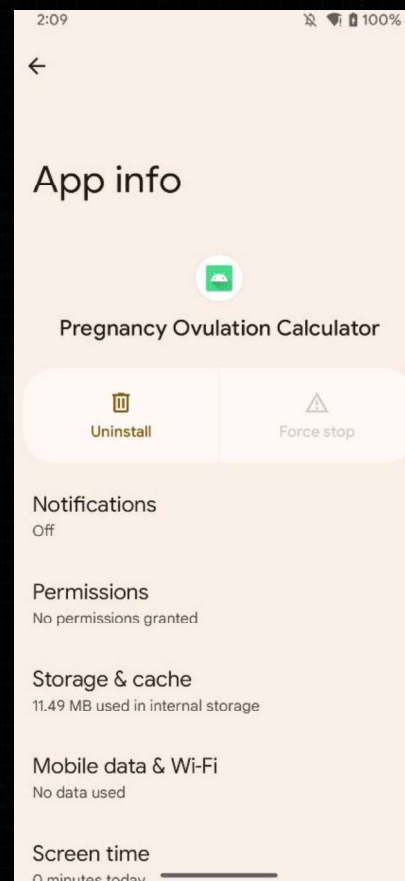


Decoy & Evil Twin App Info

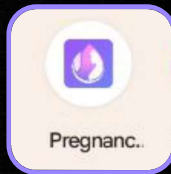
DECOY TWIN



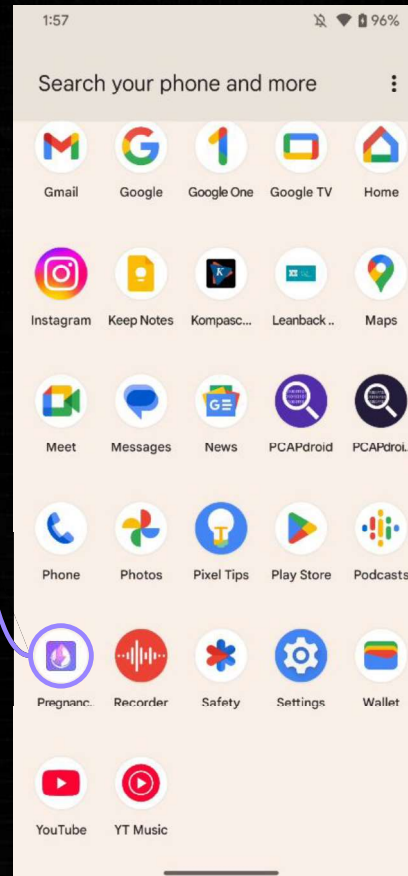
EVIL TWIN



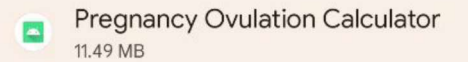
DECOY TWIN



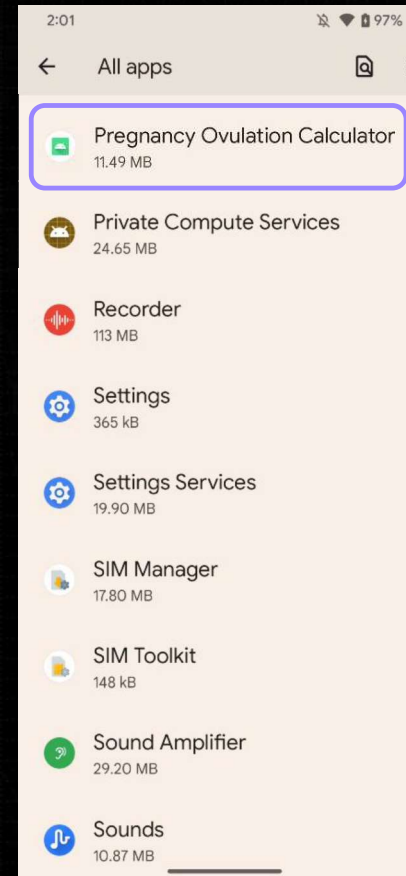
Has an app icon



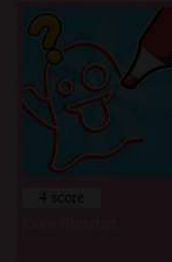
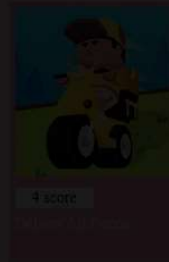
EVIL TWIN



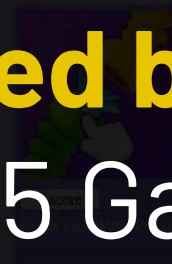
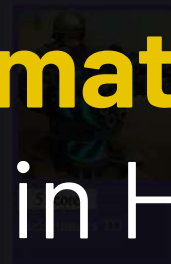
Only way to "see" Evil Twin hidden app is in "All apps"; **no app icon**



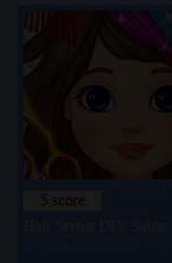
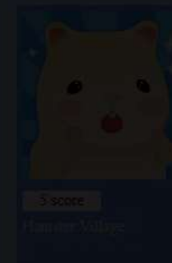
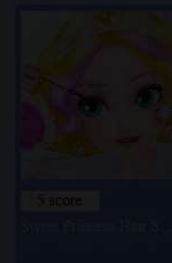
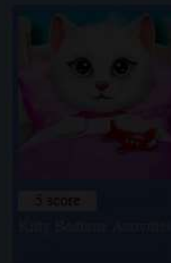
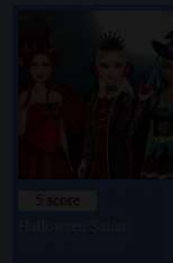
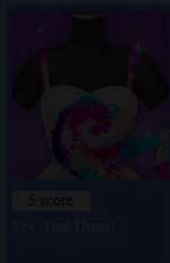
HOT GAMES



NEW GAMES

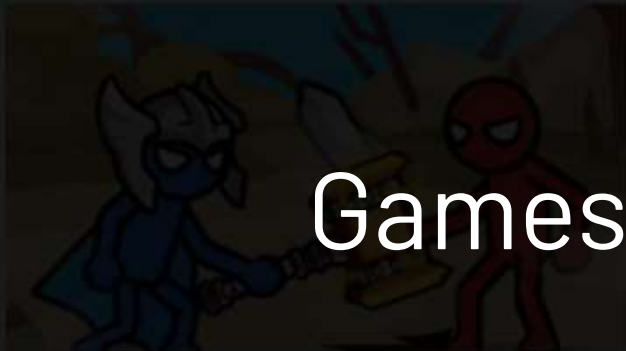


POPULAR GAMES



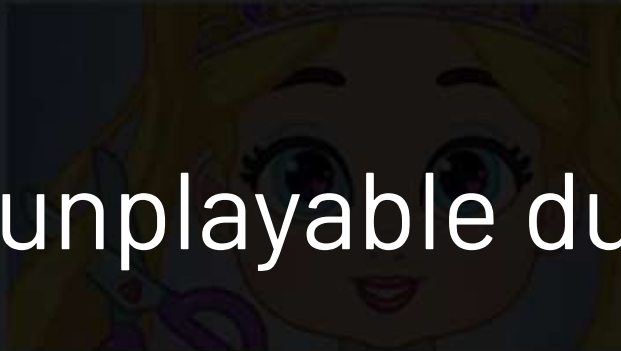
**Hidden webviews
or automated browsing
loads in H5 Games...**

Kids

[More Games](#)

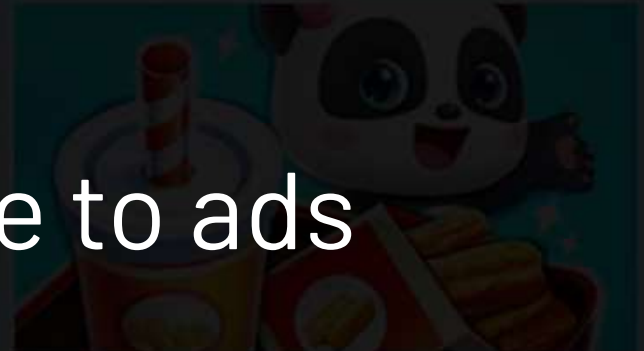
Stick Legion

1000000



Love Baby Fashion Makeover

1000000



Baby Panda Breakfast Cooking

1000000



Toddler Coloring Game

1000000



Birthday Cake For My Boyfriend

1000000



Stone Grass

1000000

Games unplayable due to ads

BADBOX 2.0 Threat Actors
**operate nearly 1000
ad-heavy gaming websites**
used as a cashout mechanism

Click Fraud

BADBOX 2.0-infected devices could be **tasked to visit low-quality domains** managed by MoYu, where they were directed to **click on the ads hosted there.**



POSTINGAN TERBARU

Seni Rupa



Seni Abstrak dalam Meningkatkan Inovasi Kreatif di Berbagai Bidang

Seni Abstrak dalam Meningkatkan Inovasi Kreatif di Berbagai Bidang - Seni abst...

Seni Rupa



Mengenal Teknik Apresiasi Seni Rupa 2 Dimensi Perspektif Hingga Kontras

Mengenal Teknik Apresiasi Seni Rupa 2 Dimensi Perspektif Hingga Kontras - Seni...

Seni Rupa



Apresiasi Seni Rupa 2 Dimensi Memahami Dimensi dan Estetis dalam Karya Visual

Apresiasi Seni Rupa 2 Dimensi Memahami Dimensi dan Estetis dalam Karya Visual ...

Seni Rupa



Sejarah dan Identitas Keunikan yang Membaur dalam Lagu Nasional

Indonesia

Sejarah dan Identitas Keunikan yang Membaur dalam Lagu Nasional Indonesia - Lagu nasional Indonesia, "Indonesia Raya," memiliki k...



Sejarah dan Karakteristik Eksplorasi Gerakan Tari Gambyong Tradisi Jawa

Surakarta

Memahami Sejarah dan Karakteristik Eksplorasi Gerakan Tari Gambyong Tradisi Jawa Surakarta - Tari Gambyong merupakan salah satu bentuk tari...



Alat, Bahan Dan Langkah Membuat Patung Dari Tanah Liat

Alat, Bahan Dan Langkah Membuat Patung Dari Tanah Liat - Membuat patung dapat dikerjakan dengan membutsir yaitu membuat bentuk karya seni...



Patung Gips - Bahan dan Teknik Cara Membuat Patung (Gypsum)

Patung Gips - Bahan dan Teknik Cara Membuat Patung (Gypsum) - Sejak zaman dulu benda-

vueling

Santiago (SCQ) ✈️ Lanzarote (ACE)

Desde...

Reserva...

vueling

Barcelona (BCN) ✈️ Lisboa (LIS)

Desde 17 €

Reserva

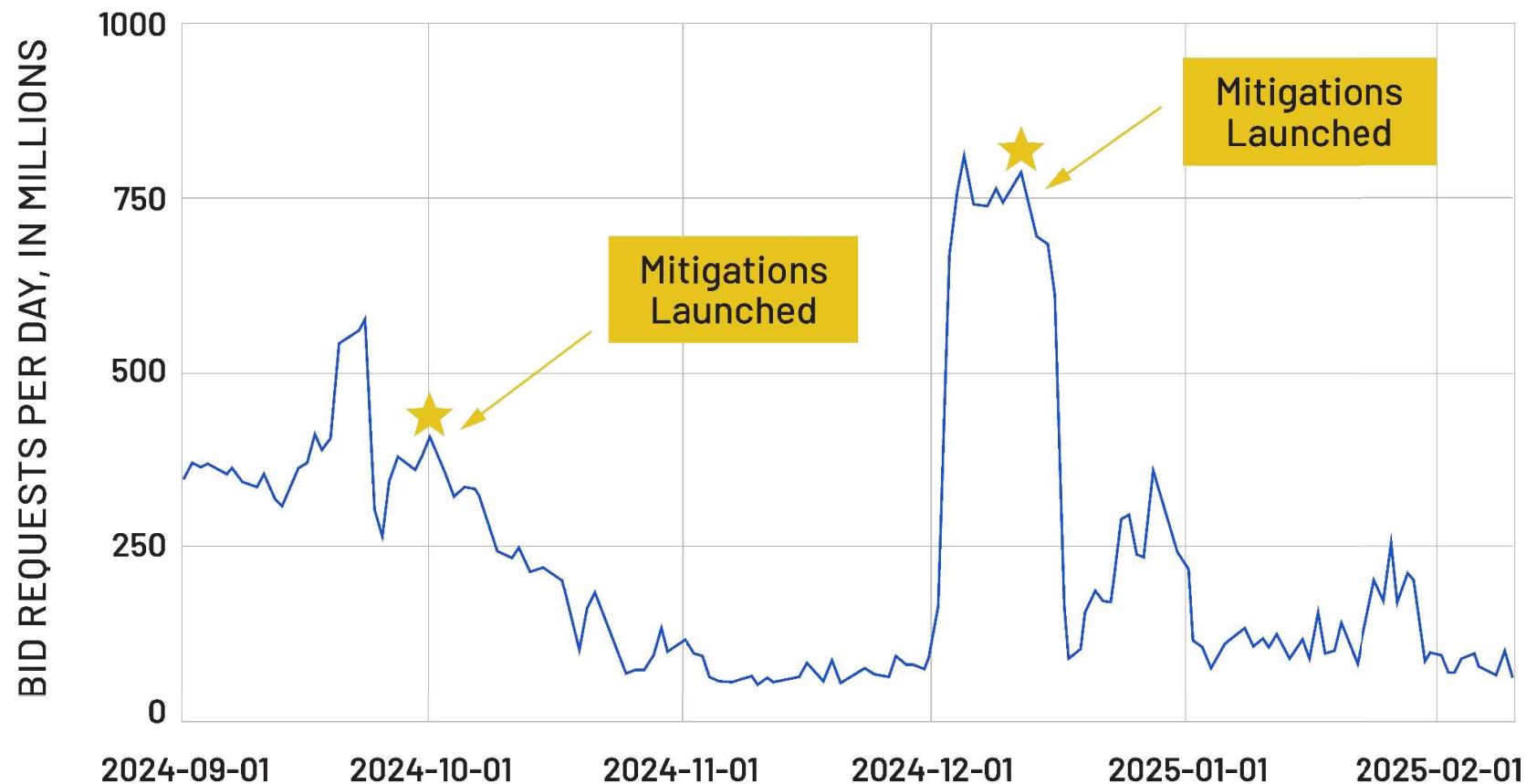
vueling

Barcelona (BCN) ✈️ Londres (LON)

Desde 25 €



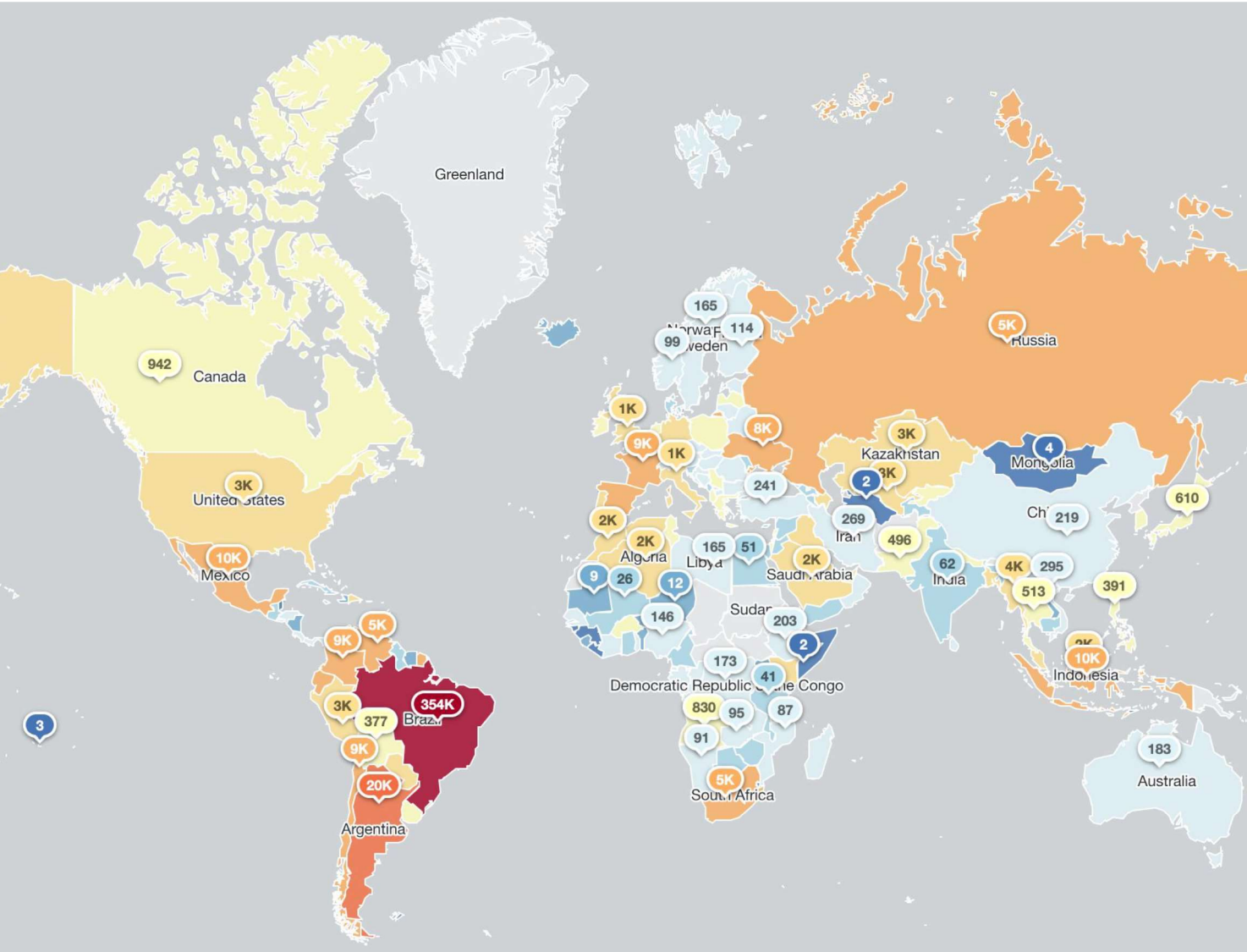
Disruption Phase 1: Reducing Profitability



Disruption Phase 2

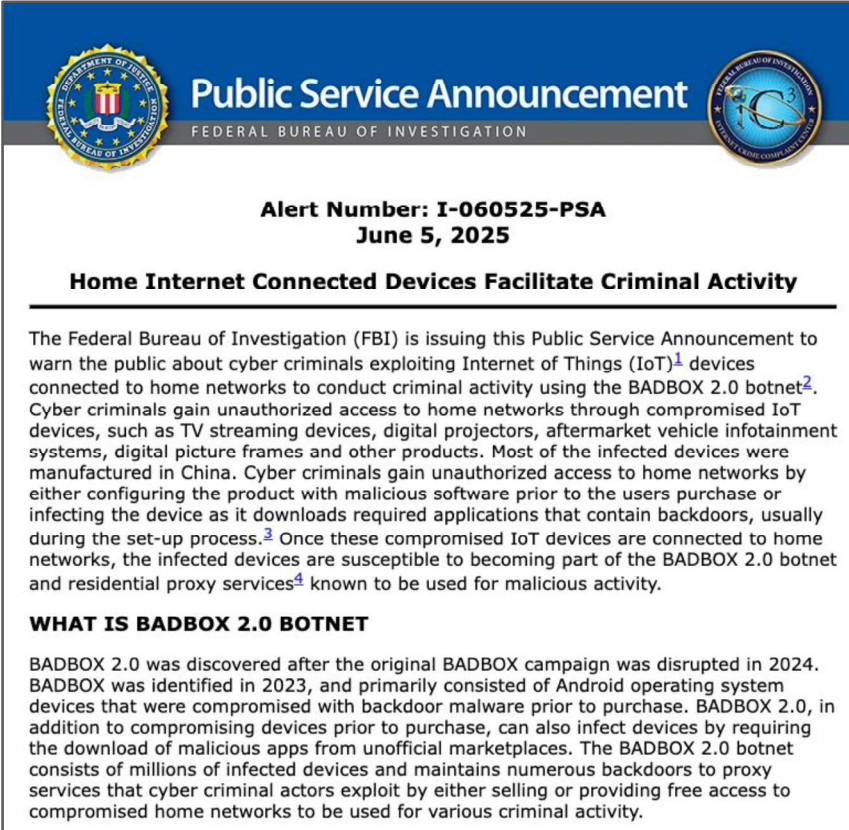
Domain Sinkholing: numbers of BADBOX 2.0's that are now not being controlled

Thanks to help from



Current Disruption Activity

- June: FBI PSA published warning about the BADBOX 2.0 threat
- July: Google publicly discloses lawsuit against 25 unnamed individuals in China associated with BADBOX 2.0
- To date, the BADBOX 2.0 botnet compromised over 10 million Android AOSP devices



The graphic is a Public Service Announcement from the Federal Bureau of Investigation (FBI). It features the FBI seal on the left and a circular logo on the right. The text is centered and includes the following information:

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-060525-PSA
June 5, 2025

Home Internet Connected Devices Facilitate Criminal Activity

The Federal Bureau of Investigation (FBI) is issuing this Public Service Announcement to warn the public about cyber criminals exploiting Internet of Things (IoT)¹ devices connected to home networks to conduct criminal activity using the BADBOX 2.0 botnet². Cyber criminals gain unauthorized access to home networks through compromised IoT devices, such as TV streaming devices, digital projectors, aftermarket vehicle infotainment systems, digital picture frames and other products. Most of the infected devices were manufactured in China. Cyber criminals gain unauthorized access to home networks by either configuring the product with malicious software prior to the users purchase or infecting the device as it downloads required applications that contain backdoors, usually during the set-up process.³ Once these compromised IoT devices are connected to home networks, the infected devices are susceptible to becoming part of the BADBOX 2.0 botnet and residential proxy services⁴ known to be used for malicious activity.

WHAT IS BADBOX 2.0 BOTNET

BADBOX 2.0 was discovered after the original BADBOX campaign was disrupted in 2024. BADBOX was identified in 2023, and primarily consisted of Android operating system devices that were compromised with backdoor malware prior to purchase. BADBOX 2.0, in addition to compromising devices prior to purchase, can also infect devices by requiring the download of malicious apps from unofficial marketplaces. The BADBOX 2.0 botnet consists of millions of infected devices and maintains numerous backdoors to proxy services that cyber criminal actors exploit by either selling or providing free access to compromised home networks to be used for various criminal activity.



HUMAN'S Satori Team

Past GLOBAL Botnet Takedowns

PARETO

6,000

The PARETO operators spoofed more than 6,000 CTV apps as part of their scheme.

1 MILLION

PARETO operated chiefly through a botnet of nearly one million infected Android phones.

650 MILLION

Across its mobile and CTV-centric botnet, the PARETO operation made more than 650 million fraudulent bid requests a day.

ICEBUCKET

28%

At its height, the ICEBUCKET scheme accounted for 28% of all connected TV traffic passing through the Human Verification Engine.

1.9 BILLION

Nearly two billion pre-bid ad requests were associated with the ICEBUCKET operation every day before its disruption.

2 MILLION

More than two million people in 30 countries were spoofed or faked during ICEBUCKET.

3ve

700,000

The 3ve botnet had more than 700,000 active infections at a time during its operation.

3 BILLION

More than 3 billion ad requests every day were attributable to the 3ve botnet.

20+

The industry group built to disrupt—and take down—the 3ve botnet and scheme was composed of more than 20 organizations, including Google, Facebook, Amazon, and the FBI.

Methbot

300 MILLION

At its zenith, the Methbot operation was "watching" 300 million video ads a day. And as video advertising carries a significantly higher cost than traditional banner or social ads, this adds up fast.

6,000

More than 6,000 premium publishers were spoofed in this operation.

10

The ringleader of the Methbot scheme was recently sentenced to 10 years in prison and restitution fines of more than \$3.5 million.

Scylla

13M+

Associated apps were downloaded 13+ million times.

80+

80 Android apps on the Google Play Store and 9 apps on the Apple App Store were affected.

Full Takedown

was orchestrated in collaboration with Google and Apple.

VASTFLUX

12 BILLION

12 billion fraudulent ad requests in one day.

11 MILLION

11 million devices running ads within apps.

1,700+

More than 1,700 apps were spoofed across platforms.

BADBOX

280,000

280,000 unique devices were impacted through ad fraud scheme.

74,000+

Over 74,000 off-brand Android devices showed signs of BADBOX infection.

227

The ad fraud botnet's conglomerate of associated apps were found in 227 countries and territories.

KONFETY

10 BILLION

At peak the malicious apps generated 10 BILLION fraudulent ad requests per day.

250 DECOY "EVIL TWIN" APPS

Satori researchers identified more than 250 app pairs abusing the CaramelAds advertising SDK across the internet.

700 URLS+

Researchers gained a broader understanding of the threat's scope from a collection of IOCs, which included over 700 URLs, likely featuring compromised free content uploaded to platforms

Phish 'n' Ships

10 MILLION

10's of millions in monetary loss for businesses and customers. Dozens of store fronts all taken down by HUMAN partners.

1,000+

Over 1,000 web pages have been infected, driving traffic to fake web shops by injecting malicious payloads into legitimate websites.

200+

200+ fake web shops that abuse digital payment providers to steal consumers' money and credit card information; 121 active during our investigation