HUMAN

UNPACKING BADBOX & DISCOVERING PEACHPIT

A Satori Threat Intelligence Team Investigation & Disruption

HUMAN's Satori Threat Intelligence and Research team announced the disruption of the PEACHPIT ad fraud botnet and their research into the larger BADBOX fraud empire. Let's unpack what we discovered.

WHAT IS BADBOX?

BADBOX is a complex threat actor scheme that begins with malware deployed on physical off-brand Android devices (TVs, cellphones, tablets) along the supply chain process in China.

TRIADA is the malware of choice used to get BADBOX into these off-brand devices.

Our team's investigation of the PEACHPIT ad fraud botnet led us to discover a connection with BADBOX. HUMAN's Satori Threat Intelligence and Research Team observed more than 74,000 Android-based mobile phones, tablets, and CTV boxes showing signs of infection.

WHAT IS PEACHPIT?

installed more than 15,000,000 times

PEACHPIT is an ad fraud branch that comes from the root of the BADBOX tree.

The PEACHPIT botnet's conglomerate of associated apps were found in 227 COUNTRIES AND TERRITORIES, with an estimated peak of 121,000 DEVICES a day on Android and 159,000 DEVICES a day on iOS.

The collection of 39 ANDROID, IOS, AND CTV-CENTRIC APPS impacted by the scheme were INSTALLED MORE THAN 15 MILLION TIMES before the apps were taken down.

WHO IS IMPACTED?

BADBOX affects consumers from both the public and private sector.

If left unchecked, the PEACHPIT ad fraud linked to BADBOX would continue to expand.

HUMAN's visibility allowed us to IDENTIFY MORE THAN 200 POTENTIALLY IMPACTED DEVICE TYPES.

Of the devices HUMAN acquired from online retailers, 80% were infected with BADBOX.

THE TIMELINE

2016
BADBOX began to be reported using blindspots in the supply chain to put Triada malware in devices.

2019
The fraudsters behind BADBOX began to test out ad fraud, but did not scale up.

2022
The ad fraud was discovered by HUMAN to have become more sophisticated by our threat hunters and coined as PEACHPIT.

2023
The PEACHPIT botnet is disrupted by the Satori Team.

HOW HUMAN IS DISRUPTING PEACHPIT:

PEACHPIT Volume Over Time

Our process involves checking for adapted and recurring threats.

OUR VISIBILITY AND EXTENSIVE DATA RESOURCES led us to uncover the PEACHPIT ad fraud botnet, and subsequently the BADBOX operation.

Once identified, WE WORKED WITH INDUSTRY PARTNERS TO DISRUPT the PEACHPIT threat in real time and protect our customers. This is the result of modern defense at work.

We've shared this information with the Human Collective and our extended network to achieve a widespread disruption of PEACHPIT.

We've given law enforcement our findings into the BADBOX operation.

Expand, profit, divide, and conquer.

That is the BADBOX methodology.

Visibility, network effect, and disruptions.

That is the HUMAN methodology.

The disruption of PEACHPIT is a major blow to the bad actors behind BADBOX and their ability to monetize their schemes.
This is how you disrupt the economics of cybercrime.

HUMAN

Learn more at humansecurity.com.