13
Trackers
Adobe Audience Manager
Adobe Dynamic Tag Management
Amazon Associates
DoubleClick
Google Analytics
Google Publisher Tags
Index Exchange (Formerly Casale Media)
New Relic
Outbrain
Parse.ly
Rubicon
ScoreCard Research Beacon
Yieldbot

SIGN IN

RISK ASSESSMENT —

More than 400 malicious apps infiltrate Google Play

"DressCode" apps turned phones into listening posts that could bypass firewalls.

DAN GOODIN - 9/30/2016, 5:05 PM

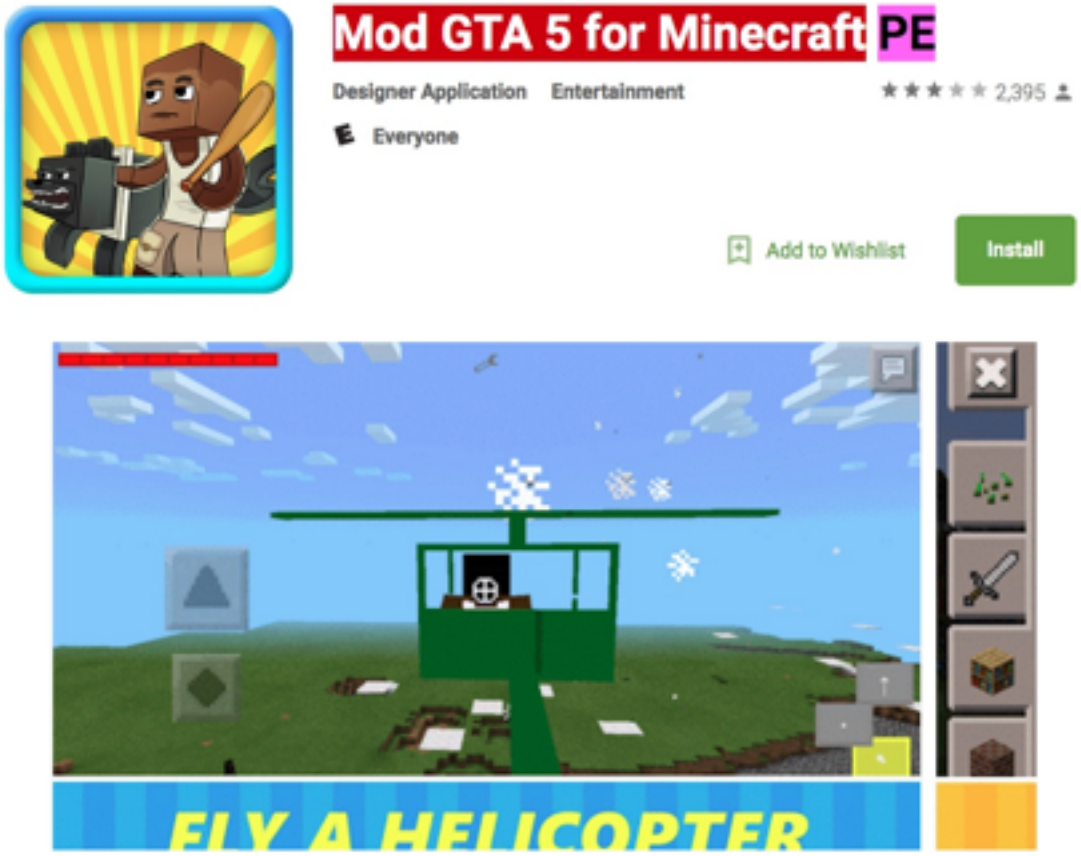
Curious Expeditions

Enlarge

78

Google Play was recently found to be hosting more than 400 apps that turned infected phones into listening posts that could siphon sensitive data out of the protected networks they connected to, security researchers said Thursday.

One malicious app infected with the so-called DressCode malware had been downloaded from 100,000 to 500,000 times before it was removed from the Google-hosted marketplace, Trend Micro researchers said in a post. Known as Mod GTA 5 for Minecraft PE, it was disguised as a benign game, but included in the code was a component that established a persistent connection with an attacker controlled server. The server then had the ability to bypass so-called network address translation protections that shield individual devices inside a network. Trend Micro has found 3,000 such apps in all, 400 of which were available through Play.



Enlarge

"This malware allows threat actors to infiltrate a user's network environment," Thursday's report stated. "If an infected device connects to an enterprise network, the attacker can either bypass the NAT device to attack the internal server or download sensitive data using the infected device as a springboard."

The report continued:

> The malware installs a SOCKS proxy on the device, building a general purpose tunnel that can control and give commands to the device. It can be used to turn devices into bots and build a botnet, which is essentially a network of slave devices that can be used for a variety of schemes like distributed denial-of-service (DDoS) attacks—which have become an increasingly severe problem for organizations worldwide—or spam email campaigns. The botnet can use the proxied IP addresses also generated by the malware to create fake traffic, disguise ad clicks, and generate revenue for the attackers.

A Google spokesman said in an e-mail: "We're aware of the issue and we're taking the necessary actions."

Trend Micro's report comes three weeks after researchers from separate security firm Checkpoint said they detected 40 DressCode-infected apps in Google Play.

Trend said that only a small portion of each malicious app contained the malicious functions, a feature that makes detection difficult. In 2012, Google introduced a cloud-based security scanner called Bouncer that scours Play for malicious apps. Since then, thousands of malicious apps have been detected by researchers. This raises a question: if outside parties can find them, why can't Google find them first?

FURTHER READING

Two critical bugs and more malicious apps make for a bad week for Android

Post updated to add comment from Google.</em?

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL *dan.goodin@arstechnica.com* // ***TWITTER*** *@dangoodin001*

READER COMMENTS 78 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Sponsored Stories

Powered by

What One Longevity Scientist Discovered About What We Need As We Age

Scientific American

This Millennial Physics Genius Is Being Hailed As The Next Einstein

Scribol

Did You Know This Is Why Marisa Tomei Never Married Anyone?

AmericanUpbeat.com

How 2 MIT Grads Are Disrupting the Auto Insurance Industry

LiveSmarterDaily

10 Rarely Seen History Photos

goodmad

Enter Your Name, Wait 14 Seconds, Brace Yourself

TruthFinder

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS