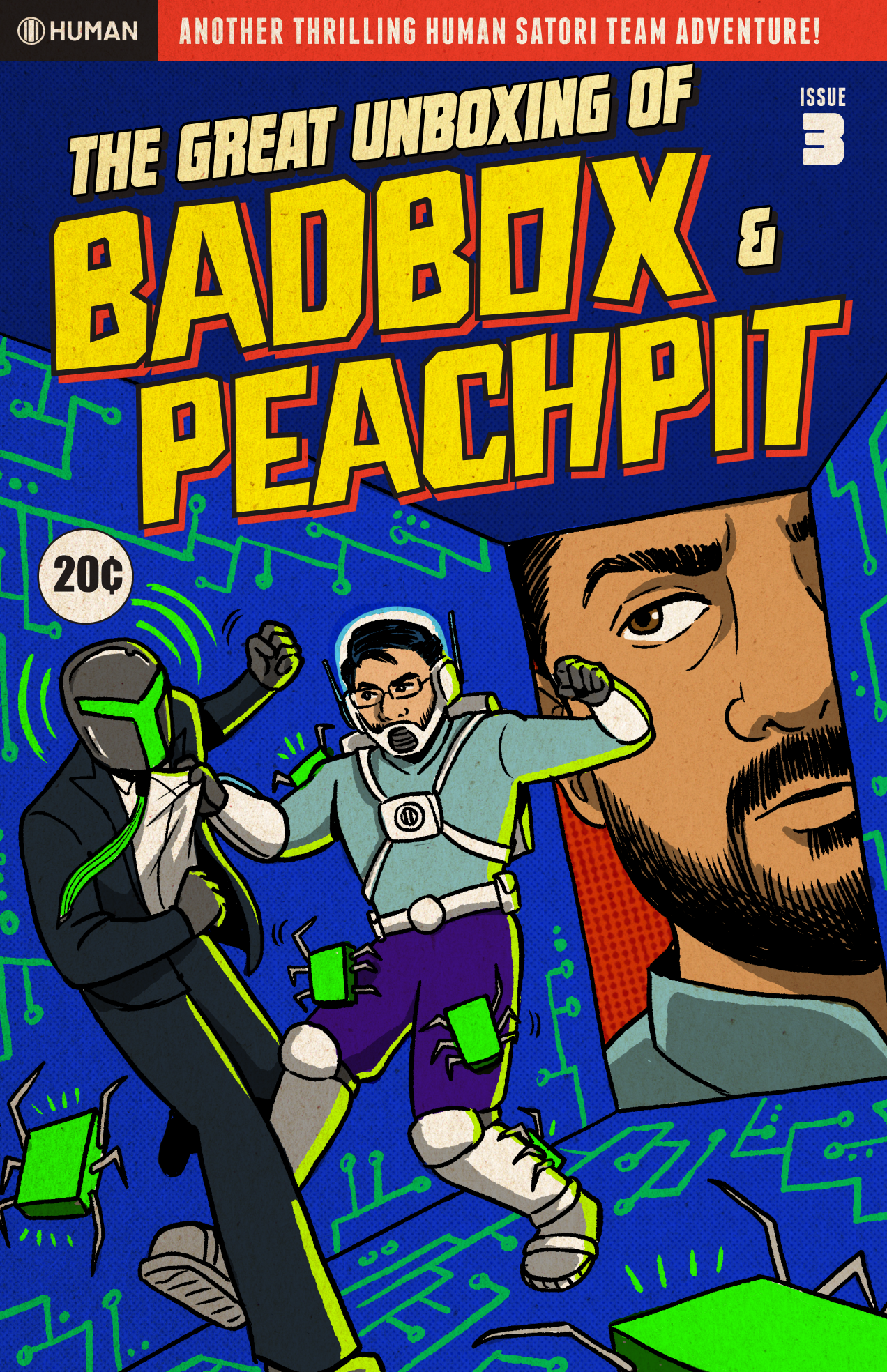
HUMAN

ANOTHER THRILLING HUMAN SATORI TEAM ADVENTURE!

ISSUE 3

THE GREAT UNBOXING OF BADBOX & PEACHPIT

20¢



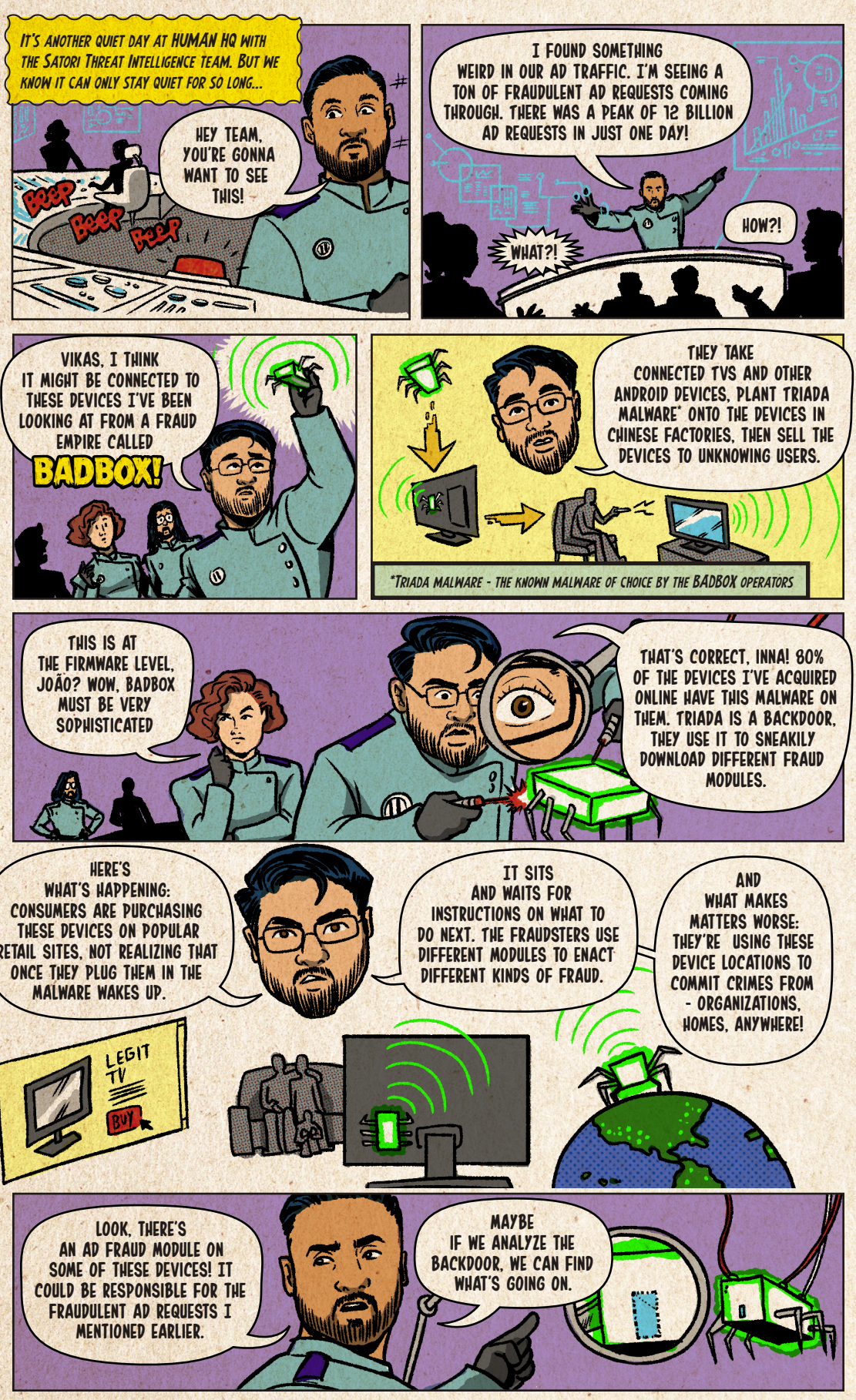
We'd like to thank the real humans of the Satori team for their work in uncovering BADBOX and disrupting Peachpit:

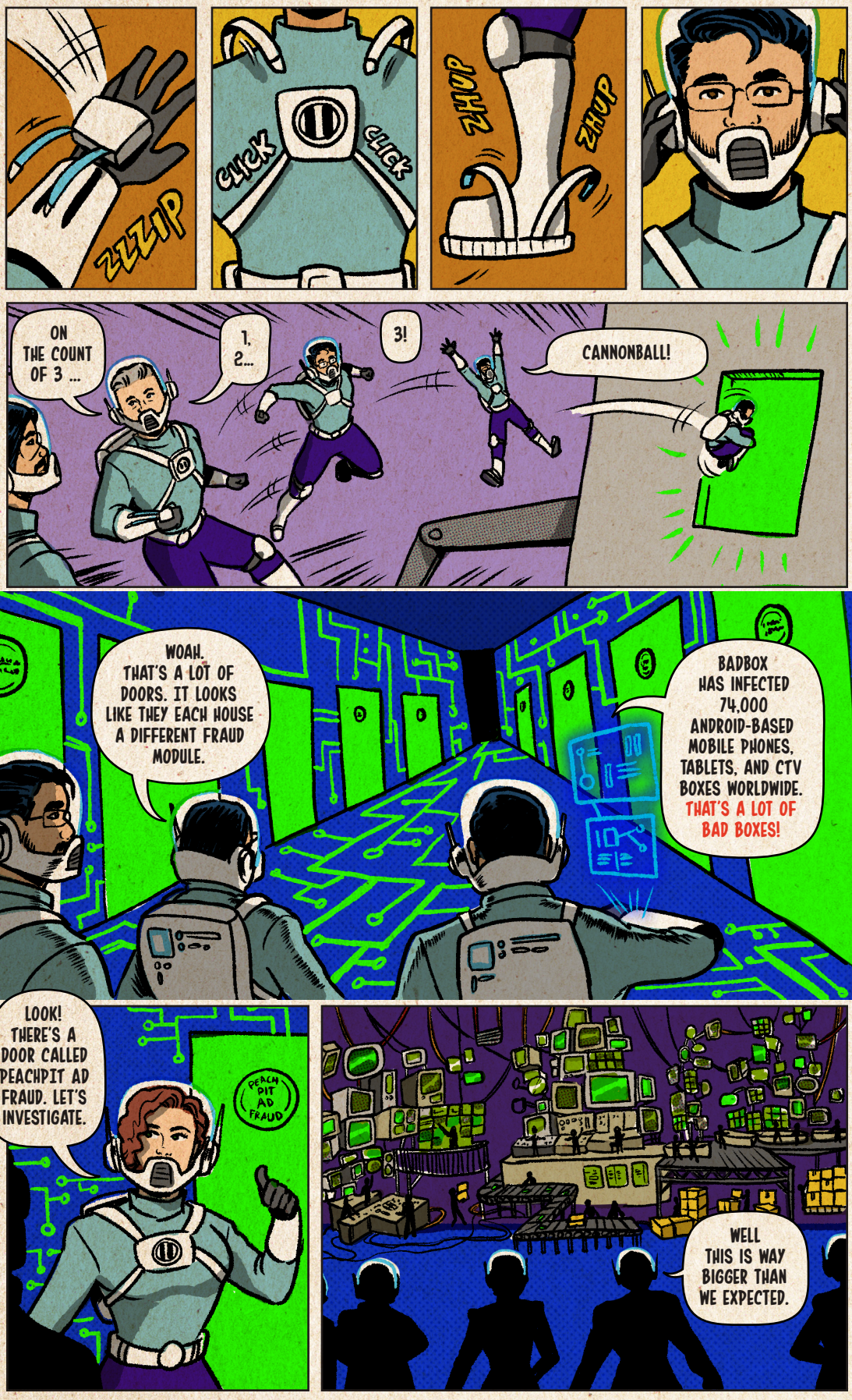
João Santos
Vikas Parthasarathy
Inna Vasilyeva
Joao Marques
Maor Elizen
Gabi Cirlig
Lindsay Kaye
Gavin Reid

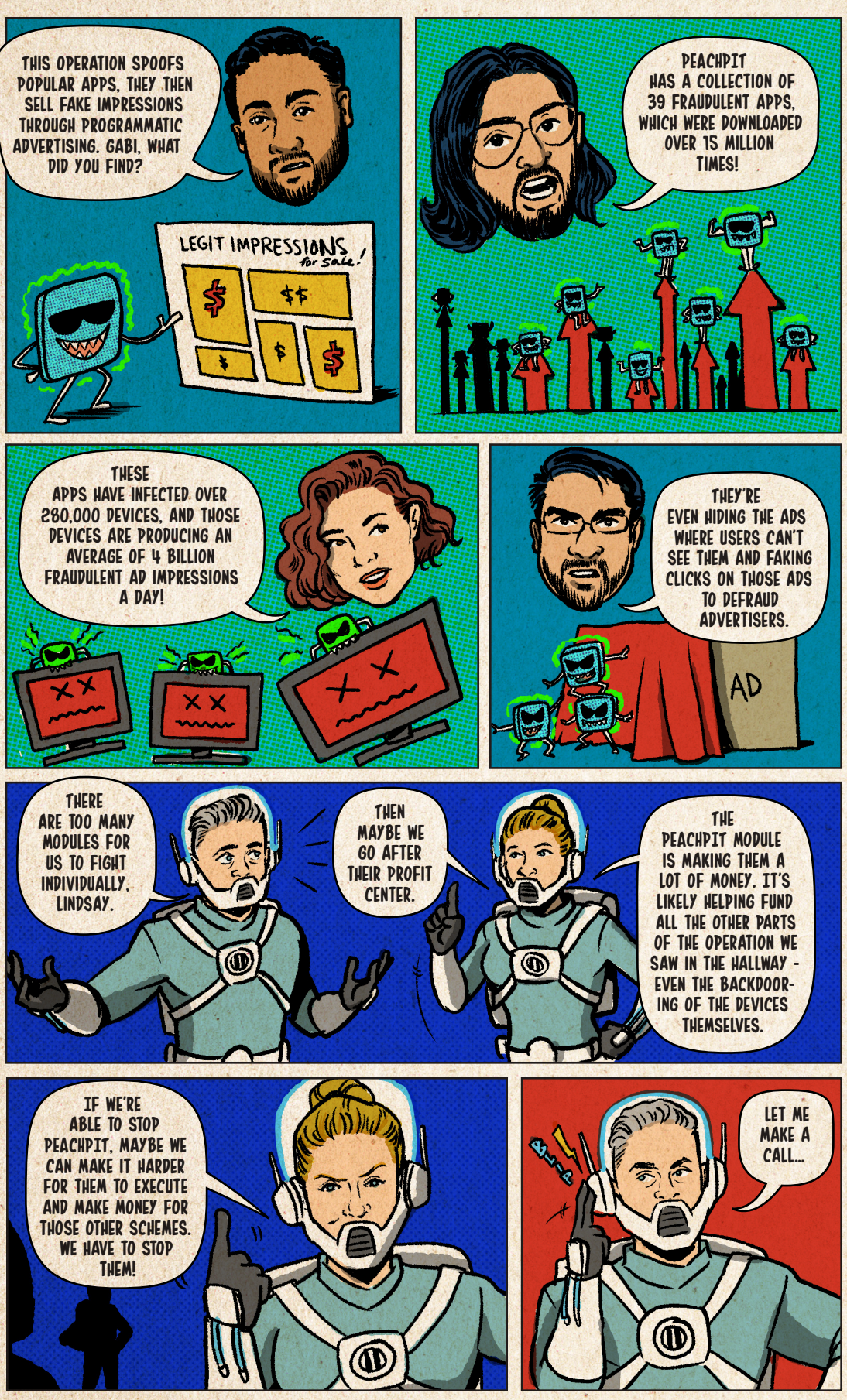
Written by:
Rosemary Cipriano

Illustrations by:
Cheyne Gallarde

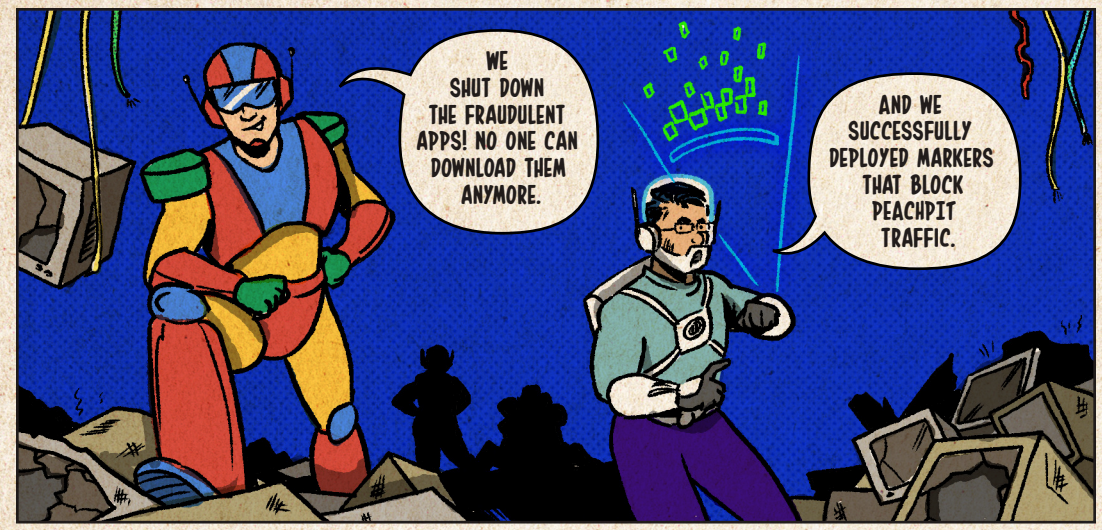
Art direction by:
Jessica Yeung

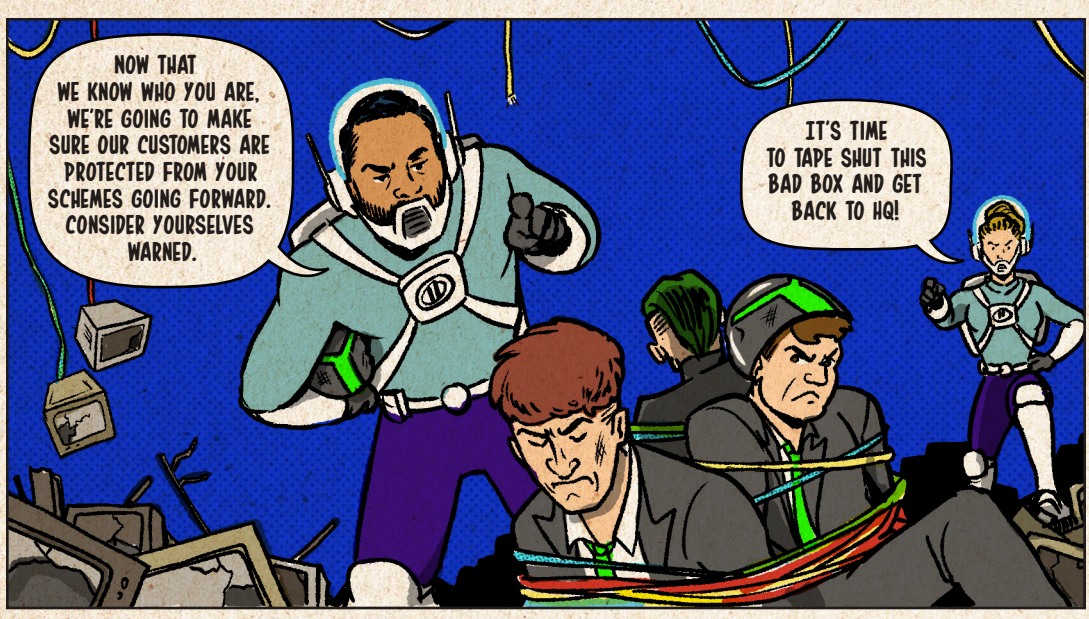

IT'S ANOTHER QUIET DAY AT HUMAN HQ WITH THE SATORI THREAT INTELLIGENCE TEAM. BUT WE KNOW IT CAN ONLY STAY QUIET FOR SO LONG...
BEEP
BEEP
BEEP
HEY TEAM, YOU'RE GONNA WANT TO SEE THIS!
I FOUND SOMETHING WEIRD IN OUR AD TRAFFIC. I'M SEEING A TON OF FRAUDULENT AD REQUESTS COMING THROUGH. THERE WAS A PEAK OF 12 BILLION AD REQUESTS IN JUST ONE DAY!
WHAT?!
HOW?!
VIKAS, I THINK IT MIGHT BE CONNECTED TO THESE DEVICES I'VE BEEN LOOKING AT FROM A FRAUD EMPIRE CALLED BADBOX!
THEY TAKE CONNECTED TVS AND OTHER ANDROID DEVICES, PLANT TRIADA MALWARE* ONTO THE DEVICES IN CHINESE FACTORIES, THEN SELL THE DEVICES TO UNKNOWING USERS.
*TRIADA MALWARE - THE KNOWN MALWARE OF CHOICE BY THE BADBOX OPERATORS
THIS IS AT THE FIRMWARE LEVEL, JOÃO? WOW, BADBOX MUST BE VERY SOPHISTICATED
THAT'S CORRECT, INNA! 80% OF THE DEVICES I'VE ACQUIRED ONLINE HAVE THIS MALWARE ON THEM. TRIADA IS A BACKDOOR. THEY USE IT TO SNEAKILY DOWNLOAD DIFFERENT FRAUD MODULES.
HERE'S WHAT'S HAPPENING: CONSUMERS ARE PURCHASING THESE DEVICES ON POPULAR RETAIL SITES, NOT REALIZING THAT ONCE THEY PLUG THEM IN THE MALWARE WAKES UP.
IT SITS AND WAITS FOR INSTRUCTIONS ON WHAT TO DO NEXT. THE FRAUDSTERS USE DIFFERENT MODULES TO ENACT DIFFERENT KINDS OF FRAUD.
AND WHAT MAKES MATTERS WORSE: THEY'RE USING THESE DEVICE LOCATIONS TO COMMIT CRIMES FROM - ORGANIZATIONS, HOMES, ANYWHERE!
LEGIT TV
BUY
LOOK, THERE'S AN AD FRAUD MODULE ON SOME OF THESE DEVICES! IT COULD BE RESPONSIBLE FOR THE FRAUDULENT AD REQUESTS I MENTIONED EARLIER.
MAYBE IF WE ANALYZE THE BACKDOOR, WE CAN FIND WHAT'S GOING ON.

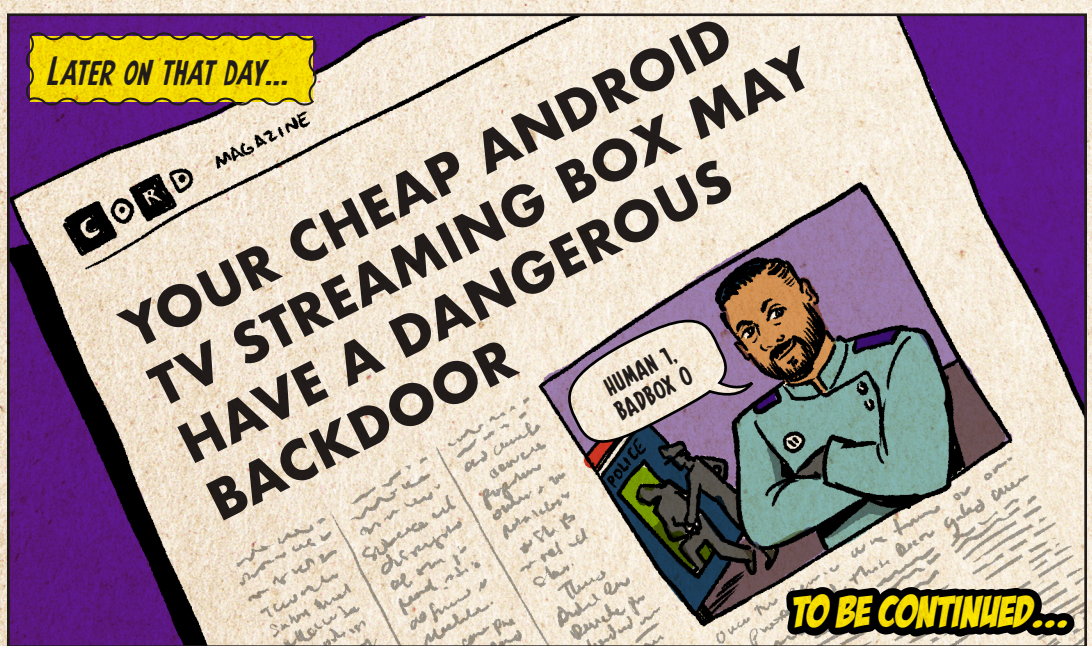

ZZZIP
CLICK
CLICK
ZHUP
ZHUP
ON THE COUNT OF 3 ...
1, 2...
3!
CANNONBALL!
WOAH. THAT'S A LOT OF DOORS. IT LOOKS LIKE THEY EACH HOUSE A DIFFERENT FRAUD MODULE.
BADBOX HAS INFECTED 74,000 ANDROID-BASED MOBILE PHONES, TABLETS, AND CTV BOXES WORLDWIDE. THAT'S A LOT OF BAD BOXES!
LOOK! THERE'S A DOOR CALLED PEACHPIT AD FRAUD. LET'S INVESTIGATE.
PEACH PIT AD FRAUD
WELL THIS IS WAY BIGGER THAN WE EXPECTED.


THIS OPERATION SPOOFS POPULAR APPS, THEY THEN SELL FAKE IMPRESSIONS THROUGH PROGRAMMATIC ADVERTISING. GABI, WHAT DID YOU FIND?
LEGIT IMPRESSIONS for Sale!
PEACHPIT HAS A COLLECTION OF 39 FRAUDULENT APPS, WHICH WERE DOWNLOADED OVER 15 MILLION TIMES!
THESE APPS HAVE INFECTED OVER 280,000 DEVICES, AND THOSE DEVICES ARE PRODUCING AN AVERAGE OF 4 BILLION FRAUDULENT AD IMPRESSIONS A DAY!
THEY'RE EVEN HIDING THE ADS WHERE USERS CAN'T SEE THEM AND FAKING CLICKS ON THOSE ADS TO DEFRAUD ADVERTISERS.
AD
THERE ARE TOO MANY MODULES FOR US TO FIGHT INDIVIDUALLY, LINDSAY.
THEN MAYBE WE GO AFTER THEIR PROFIT CENTER.
THE PEACHPIT MODULE IS MAKING THEM A LOT OF MONEY. IT'S LIKELY HELPING FUND ALL THE OTHER PARTS OF THE OPERATION WE SAW IN THE HALLWAY - EVEN THE BACKDOORING OF THE DEVICES THEMSELVES.
IF WE'RE ABLE TO STOP PEACHPIT, MAYBE WE CAN MAKE IT HARDER FOR THEM TO EXECUTE AND MAKE MONEY FOR THOSE OTHER SCHEMES. WE HAVE TO STOP THEM!
LET ME MAKE A CALL...

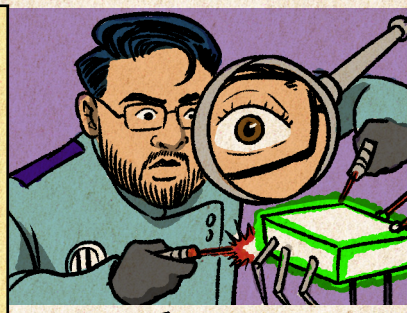

IT'S WORSE THAN WE THOUGHT. CAN YOU SEND REINFORCEMENTS?
YES! I'M CALLING ON THE HUMAN COLLECTIVE!
PARTNERS!
CUSTOMERS!
POW!
SMAASH!
CRAAASH!


WE SHUT DOWN THE FRAUDULENT APPS! NO ONE CAN DOWNLOAD THEM ANYMORE.
AND WE SUCCESSFULLY DEPLOYED MARKERS THAT BLOCK PEACHPIT TRAFFIC.


NOW THAT WE KNOW WHO YOU ARE, WE'RE GOING TO MAKE SURE OUR CUSTOMERS ARE PROTECTED FROM YOUR SCHEMES GOING FORWARD. CONSIDER YOURSELVES WARNED.
IT'S TIME TO TAPE SHUT THIS BAD BOX AND GET BACK TO HQ!


LATER ON THAT DAY...
CORD MAGAZINE
YOUR CHEAP ANDROID TV STREAMING BOX MAY HAVE A DANGEROUS BACKDOOR
HUMAN 1, BADBOX 0
POLICE
TO BE CONTINUED...

On October 4, 2023, HUMAN's Satori Threat Intelligence team published their findings into the BADBOX fraud empire and the subsequent disruption of the PEACHPIT ad fraud module. The BADBOX operation, based out of China, sold off-brand mobile and Connected TV (CTV) devices on popular online on retailers and resale sites. These Android devices came preloaded with a known malware called Triada. Once the device was turned on or plugged in, those devices called home and got several "modules" of fraud installed on them remotely. One of which was an ad fraud module we dubbed PEACHPIT. This cybercriminal enterprise didn't discriminate - they went after consumers around the world both in the private and public sectors. The Satori Threat Intelligence team observed more than 74,000 Android-based mobile phones, tablets, and CTV boxes showing signs of infection. 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. At its peak, PEACHPIT-associated apps appeared on 121,000 Android devices and 159,000 iOS devices in 227 countries and territories. HUMAN worked with Google and Apple to disrupt the PEACHPIT operation. HUMAN has also shared information about the facilities at which some BADBOX-infected devices were created with law enforcement, including information about the organizations and individual threat actors believed to be responsible for the PEACHPIT operation.



READY TO DIVE DEEPER?

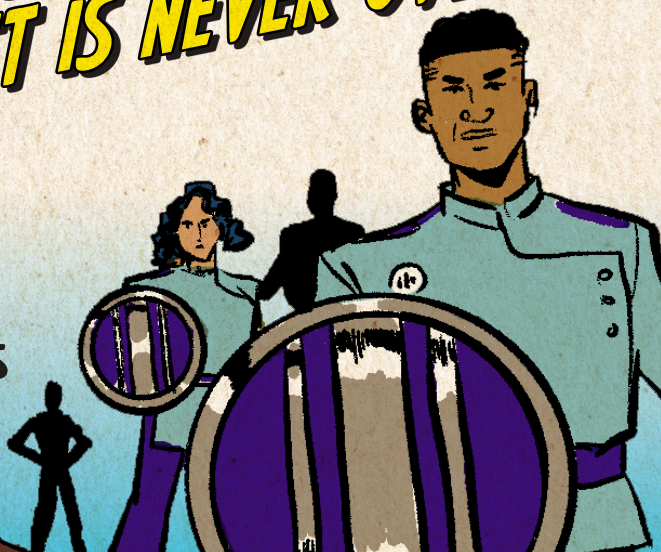
JOIN OUR TEAM!

Check out all of our resources around BadBox:

THE FIGHT FOR HUMANITY ON THE INTERNET IS NEVER OVER!

We need you to make our mission a reality. See all of our open roles at

HUMANSECURITY.COM/CAREERS



HUMAN