ANOTHER THRILLING HUMAN SATORI TEAM ADVENTURE!

THE DEEP SEA DISRUPTION

OF SCYLLA & CHARYBDIS

20¢
WE'D LIKE TO THANK THE REAL HUMANS OF THE SATORI TEAM FOR THEIR WORK IN DISRUPTING SCYLLA AND CHARYBDIS:

INNA VASILYeva
NICO AGNESE
JOAO SANTOS

VIKAS PARTHASARATHY
MARION HABIBY

AND MANY MORE BRAVE HUMANS

WRITTEN BY:
ROSEMARY CIPRIANO

ILLUSTRATIONS BY:
CHEYNE GALLARDE

ART DIRECTION BY:
JESSICA YEUNG
It was a typical day in the office for HUMAN’s Satori Threat Intelligence & Research team... until their monitors glowed with a new fraud they found.

Remember when we disrupted an ad fraud operation in 2019 called Poseidon? I think they're back.

Well for starters, they’re using code obfuscation to hide the fraud inside... new apps!

I did some reverse engineering and discovered they’re targeting specific advertising platforms and systems.

The threat is called: Charybdis

That’s not all! I also found 75 Android apps and 10 iOS apps committing ad fraud connected to these fraudsters.

These apps generated 13 million downloads in total so far!

This is called Scylla. It’s the same threat actors for both.

Hey everyone, I think you’re gonna want to see this.

But the malicious apps were removed! What are they doing now?

“Poseidon - A collection of 40 Android apps openly committing multiple types of advertising fraud, such as out-of-context ads and hidden ads. It was no match for the Satori team, who worked with Google to remove the apps from the Play Store.”

Hey everyone, I think you're gonna want to see this.

Remember when we disrupted an ad fraud operation in 2019 called Poseidon? I think they're back.

Well for starters, they’re using code obfuscation to hide the fraud inside... new apps!

I did some reverse engineering and discovered they’re targeting specific advertising platforms and systems.

The threat is called: Charybdis

That’s not all! I also found 75 Android apps and 10 iOS apps committing ad fraud connected to these fraudsters.

These apps generated 13 million downloads in total so far!

This is called Scylla. It’s the same threat actors for both.

But just like last time, they won’t get away with it.
This is where we disrupted Poseidon in 2019. I wonder where they all went.

Maybe they set up camp for Charybdis and Scylla nearby...

Wait, they didn’t change the encryption string. Let’s follow it and see where it takes us!
Allatori swaps out elements of code for single letters and numbers.

They're also targeting SDKs of specific advertising platforms!

This makes it really hard for someone to look at the app code and know what it's supposed to do.

Let's split up. You investigate Charybdis. We'll check out Scylla.

Here's what we found out about Charybdis: The fraudsters are using a popular developer tool called Allatori.

Allatori swaps out elements of code for single letters and numbers.

They're also targeting SDKs of specific advertising platforms!
Meanwhile at Scylla Base...

From what we can tell, Scylla is even more sophisticated than Charybdis.

The apps and bundle I.D.s are spoofed!

"App and Bundle ID Spoofing - When an app contains code that tells advertisers and ad tech companies that it's a different app entirely, with the intent of tricking those companies into placing ads there or into spending more money to place ads. The trickery stops here!"

And to make matters worse, they're showing ads out-of-context and hidden ads, driving consumers crazy!

They're showing ads where they shouldn't be, or not at all. That's not what advertisers want!

It's worse than we thought. We need to call in our customers and partners as reinforcements!

How soon can you get here?
That's right, this Greek tragedy is over! We shut down the apps and we worked with our customers to protect the whole ecosystem.

Good job, everyone! I think it's time to get back to HQ - the fight against fraud never rests!

To be continued...
On September 23, 2022, HUMAN’s Satori Threat Intelligence & Research team announced the disruption of the ad fraud operations Charybdis and Scylla. They were adaptations of an operation disrupted back in 2019 called Poseidon. It became obvious to our researchers that the fraudsters were reading our research into them, and adapting based on those findings. However, our team was clever to not include everything they discovered which allowed them to uncover the fraudsters’ subsequent operations.

Charybdis was known for code obfuscation and SDK targeting of popular ad tech platforms. Scylla was notably much larger and more sophisticated. The Satori team uncovered a collection of 75 apps on Google’s Play Store and 10 apps on Apple’s App Store that contained obfuscated code similar to Charybdis. The Satori team worked with the Google and Apple app store teams to take down the apps, disrupting Scylla and Charybdis from impacting the programmatic advertising ecosystem and customers around the world.