

ENTRY // Xiongmai Security Research #0 // Intro

[-] [X]

Date: 2019-09-04 Author: Ian Rash Index: #0

Hello everyone, and welcome to my investigative journey into the Besder (actually Xiongmai) IP20H1 network camera! Last time, ([VStarCam Investigational Journey](#)), I covered the VStarCam C7824WIP, a fully featured network camera with some BIG custom protocol flaws. Using knowledge gained from investigation, I was able to write an "anti-client" which could pilfer the password to the camera from a client, reflect the credentials at the camera, then install our own firmware which unfortunately bricked the device. I bought a brand new device and I'm ready to try again.

After my first article, [Brian Cardiff](#) from [Manas](#), the creators of the [Crystal](#) language, reached out to me to say that they enjoyed the article and they wanted to give me a gift card to Amazon to pick out a new camera! And that's exactly what I did. Big thank you to the Crystal team for doing this, they are some wonderful people, and I'm really glad to be a part of their community!

If you would like to participate, you can buy the camera from [Amazon](#), and follow along, just be sure to follow these [guidelines](#), as the camera itself is basically a bot in a botnet.

All source code can be found on Github at [sol-vin/xiongmai-investigational-journey](#)

TAGGED SKILLS:



Security Research



Hardware Security



Reverse Engineering