PRODAFT

Threat Intelligence Insights

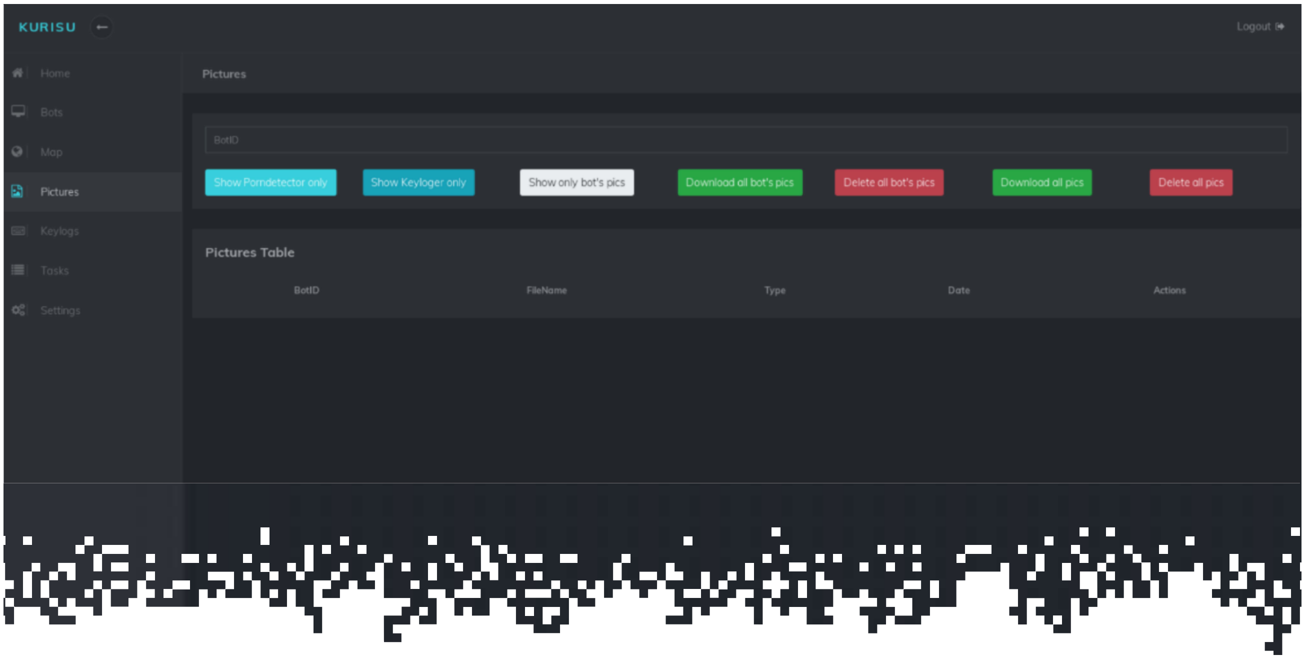
Kurisu Malware

New Kurisu Malware Used In Sextortion Campaigns

The PRODAFT Threat Intelligence (PTI) team detected a new malware that surfaced in May 2022 called *Kurisu.*

The malware has a **keylogger** functionality, meaning it's created to spy on victims and capture everything they type. Using this functionality on web-browser sessions, Kurisu can check if the infected devices are visiting adult sites and, if so, capture photos of them to later use for sextortion.

Sextortion is a form of blackmail in which a threat actor claims to possess or possesses evidence of sexual behavior from the victim. The threat actor demands payment for not spreading the compromising information, images, or videos. These campaigns can be combined with botnets, ransomware, and other methods of cyberattacks.



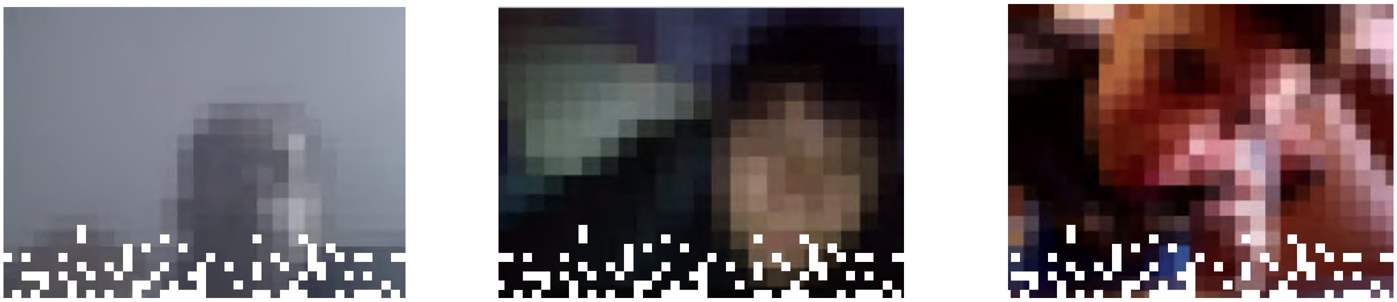
Dashboard of the Kurisu malware

The Strategy

Kurisu is distributed through a privacy-oriented browser. Threat actors trick the victims into installing the browser by highlighting its privacy-oriented features and inject the malware into it.

Once the browser is installed, the malware identifies whether the infected device is using an adult site. Kurisu opens the victim’s webcam and automatically takes photos of the victim.

The pictures are then used for sextortion, and the victims are pressured to pay a ransom.



Photos of victims captured by the Kurisu malware

The Findings

The motivation behind these attacks is financial gain. When the PTI team investigated Kurisu, the Command and Control server records contained various photos used in sextortion scams.

The investigation on Kurisu is ongoing. Our PTI team will continue to monitor the malware closely and determine additional actions as the situation requires.You can find the indicators of compromise (IOCs) from our GitHub page; we constantly update our page based on new findings.

Our threat intelligence platform monitors thousands of sources to identify and prevent these attacks quickly. With the help of the U.S.T.A. platform, you can respond to cyber security threats that come your way successfully.