Beware of BIOPASS malware hidden in Chinese online gambling sites

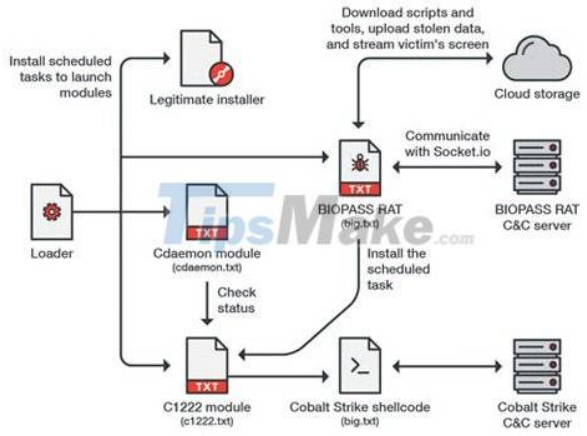
Cybersecurity researchers are warning of a new malware - BIOPASS RAT - attacking online gambling companies in China.

BIOPASS RAT takes advantage of the Open Broadcaster Software (OBS) Studio streaming application to capture victim screens.

The attack involved tricking visitors into a game website and downloading a malware loader disguised as a legitimate installer for popular but deprecated apps, like Adobe Flash Player or Microsoft Silverlight. The purpose of this is for the loader to act as a conduit to fetch the payloads for the next stage.

Specifically, the online support chat pages of online gambling sites are infected with malicious JavaScript code, which is used to spread malware to victims.

"BIOPASS RAT has basic features found in other malware, such as file system evaluation, remote desktop access, file filtering, and shell command execution," the researchers said. Trend Micro said. "It has the potential to compromise victims' personal information by stealing web browser and messaging app data."



OBS Studio is an open source video recording and live streaming software that allows users to live stream to Twitch, YouTube and other platforms.

Besides being equipped with a wide range of capabilities to run all typical spyware, BIOPASS is also equipped to set up streaming to a cloud service, under attacker control via Real- Time Messaging Protocol (RTMP), in addition to communicating with a command-and-control (C2) server using the Socket.IO protocol.

This malware is spreading aggressively. It mainly steals personal data from the most popular web browsers and messaging apps in China, including QQ Browser, 2345 Explorer, Sogou Explorer, 360 Safe Browser, WeChat, QQ and Aliwangwang.

It's unclear exactly who is behind this attack, but Trend Micro researchers say they found an overlap between BIOPASS and TTPs - related to Winnti Group (aka APT41) - a group Sophisticated Chinese hacking.

"BIOPASS RAT is a type of sophisticated malware that is deployed as Python scripts. Because the malware loader is distributed as an executable that is disguised as a legitimate update installer on the site. web is compromised, [.] you should only download apps from trusted sources and official websites to avoid being compromised,' the researchers warned.