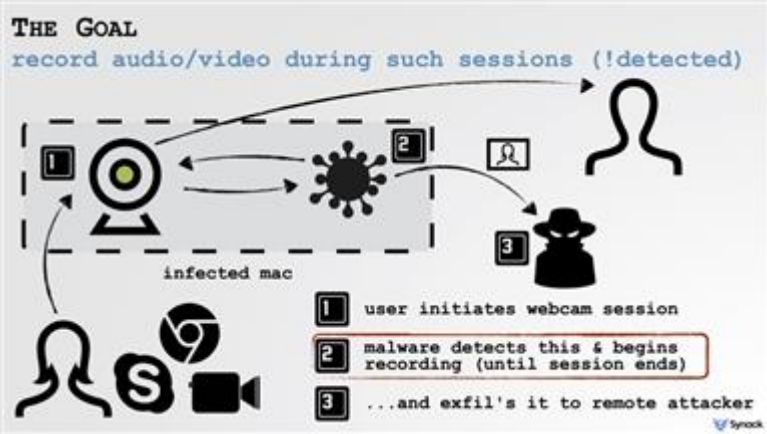
Cameras Vulnerable To Hacking During Skype Calls – World Atlantic



On October 12, 2016, research from the cyber security company Synack detailed a method used by hackers to access any virtual call made via Skype. The technique, known as "piggybacking," installs a malware program that quietly runs in the background of a computer and checks the activation of the camera periodically. When the camera is turned on, the malware starts recording either in Skype or FaceTime, and stops recording when the session ends. Finally, the malware sends the information to the attacker. According to Synack Director Patrick Wardle, the technique is virtually undetectable because the user does not note any unusual camera activity during the call. As part of the investigation, the firm creates free Mac applications that protect computers using Apple's operating systems from the problem.

Comment:

Persons using Apple's operating systems and Mac computers are encouraged to download effective antivirus or protective programs that display notifications every time a program starts recording via the webcam. Christian Aid computers should be checked regularly by the IT department to prevent any malware infections. Christian Aid Staff are recommended not to share sensitive information via virtual calls such as Skype, FaceTime, Hangout, or similar platforms. A low-price and common practice to avoid espionage through computer cameras is to cover the webcam at all times and be alert to any suspicious activity on electronic equipment.