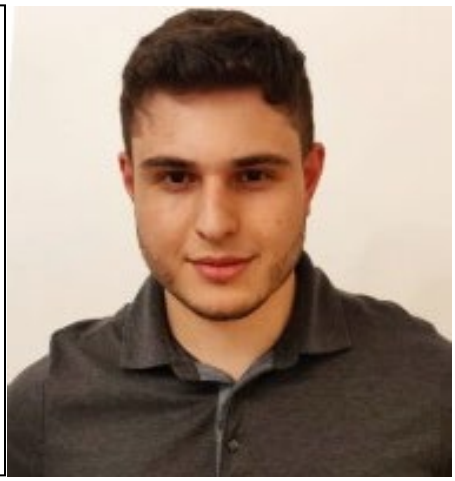
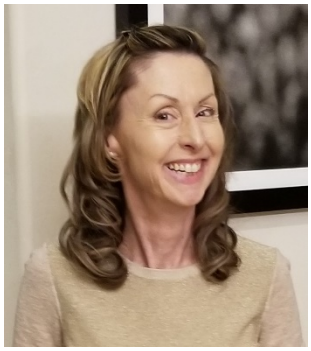
Windows Facial Recognition Authentication Hacked – Easily

In May 2020, Microsoft reported that Windows Hello had over 150M users and that 84.7% of Windows10 users sign in using Windows Hello. This vast facial recognition user base drew the interest of CyberArk. The system works only with webcams that have an infrared sensor in addition to the regular RGB sensor, but does not even look at the RGB data.

"We created a full map of the Windows Hello facial-recognition flow and saw that the most convenient for an attacker would be to pretend to be the camera, because the whole system is relying on this input." "Our findings show that any USB device can be cloned, and any USB device can impersonate any other USB device. Identifying a USB device by a descriptor provided by the device is the main reason for this. The OS cannot validate such a device authenticity, at least not according to the USB specification."
Omer Tsarfati, Cyber Security Researcher, CyberArk



By using one straight-on infrared image of a target's face and one black frame, they were able to breach Windows Hello. An attacker would have to have physical access to the device to exploit it. Microsoft immediately released patches to correct the egregious error. CyberArk provides a proof-of-concept video demonstrating how they bypassed Windows Hello. They successfully hacked the program by capturing an image of someone, saving the captured frames, impersonating a USB camera device, and sending those frames to the system for verification. Because Windows Hello relies on external data sources, the program is exploitable. Because the host cannot identify which device is connected to the USB port, each device can subversively impersonate another. CyberArk completed the breach using an accurate infrared image of its target – paired with RGB frames of SpongeBob SquarePants.



Karen Heumann, G2M Communications