



Oops!.. I Think I Scanned a Malware

Researchers

Ben Nassi
nassidt@gmail.com

Prof. Adi Shamir
adi.shamir@weizmann.ac.il

Prof. Yuval Elovici
elovici@inter.net.il

Publications

B. Nassi, A. Shamir, Y. Elovici,
“Oops!.. I think I scanned a
malware,” 2017. arXiv:1703.07751.

Description

The researchers present a proof-of-concept illustrating the feasibility of creating a covert channel between a C&C server and a malware installed in an organization by exploiting an organization’s scanner and using it as a means of interaction. We take advantage of the light sensitivity of a flatbed scanner, using a light source to infiltrate data to an organization. We present an implementation of the method for different purposes (even to trigger a ransomware attack) in various experimental setups using: (1) a laser connected to a stand (2) a laser carried by a drone, and (3) a hijacked smart bulb within the organization targeted by a passing car. In our experiments we were able to infiltrate data using different types of light sources (including infrared light), from a distance of up to 900 meters away from the scanner. We discuss potential counter measures to prevent the attack.