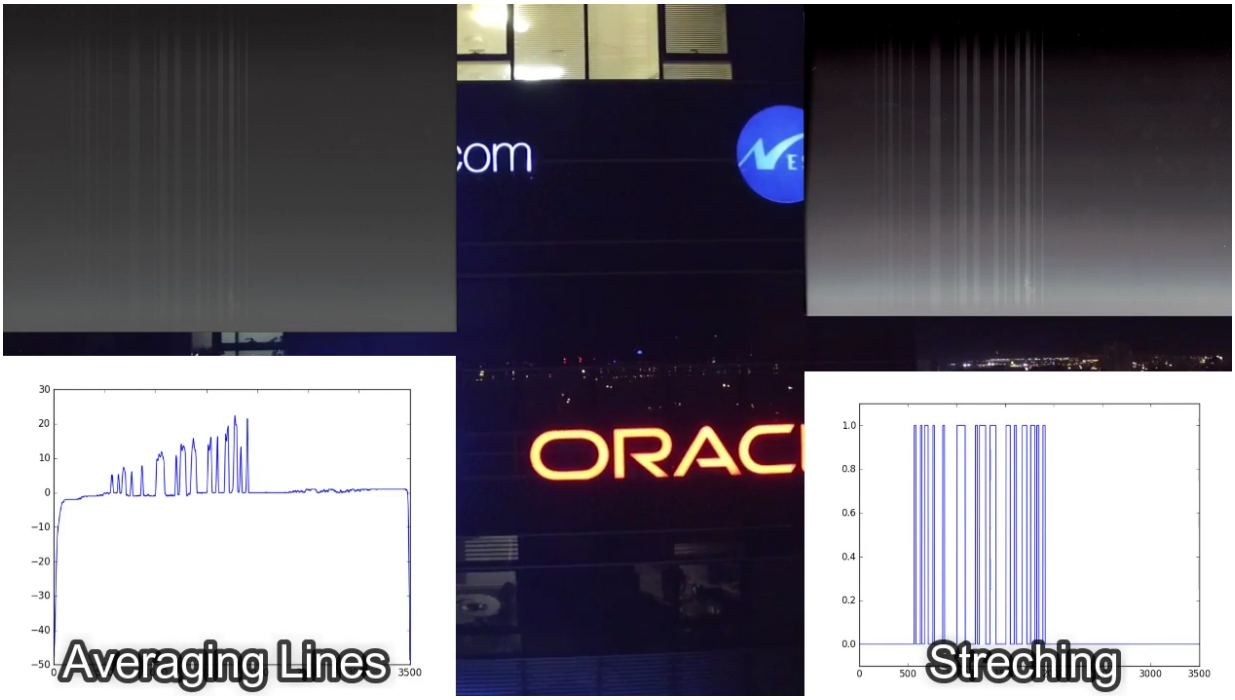
Desktop scanners can be hijacked to perpetrate cyberattacks

March 28 2017



A typical office scanner can be infiltrated and a company's network compromised using different light sources, according to a new paper by researchers from Ben-Gurion University of the Negev and the Weizmann Institute of Science.

"In the paper, "Oops! I Think I Scanned Malware," we demonstrated

how to use a laser or smart bulb to establish a covert channel between an outside attacker and malware installed on a networked computer," says lead author Ben Nassi, a graduate student in the BGU Department of Software and Information Systems Engineering as well as a researcher at the BGU Cyber Security Research Center (CSRC). "A scanner with the lid left open is sensitive to changes in the surrounding light and might be used as a back door into a company's network."

The researchers conducted several demonstrations to transmit a message into computers connected to a flatbed scanner. Using direct laser light sources up to a half-mile (900 meters) away, as well as on a drone outside their office building, the researchers successfully sent a message to trigger malware through the scanner.

In another demonstration, the researchers used a Galaxy 4 Smartphone to hijack a smart lightbulb (using radio signals) in the same room as the scanner. Using a program they wrote, they manipulated the smart bulb to emit pulsating light that delivered the triggering message in only seconds. Watch a video of the smart bulb attack.

To mitigate this vulnerability, the researchers recommend organizations connect a scanner to the network through a proxy server—a computer that acts as an intermediary—which would prevent establishing a covert channel. This might be considered an extreme solution, however, since it also limits printing and faxing remotely on all-in-one devices.

"We believe this study will increase the awareness to this threat and result in secured protocols for scanning that will prevent an attacker from establishing such a covert channel through an external light source, smart bulb, TV, or other IoT (Internet of Things) device," Nassi says.

Prof. Adi Shamir of the Department of Applied Mathematics at the Weizmann Institute conceived of the project to identify new network

vulnerabilities by establishing a clandestine channel in a computer network.

Ben Nassi's Ph.D. research advisor is Prof. Yuval Elovici, a member of the BGU Department of Software and Information Systems Engineering and director of the Deutsche Telekom Laboratories@BGU. Prof. Elovici is also director of the CSRC.

Provided by American Associates, Ben-Gurion University of the Negev