BYOD mobile attack prevention app uses machine learning

January 24 2014, by Nancy Owano

CONSOLE
MANAGEMENT
DIAGNOSTICS
PROTECTION
IPS
ANTI

(Phys.org) —Mobile security company Zimperium is introducing attack-protection software for mobile devices and they have designed the product to go where other malware-sniffing apps might not. They aim to attract today's companies increasingly involved in BYOD environments and BYOD security policy needs. Zimperium's technology, supporting Android platforms, takes the interesting approach of machine learning to sniff out and prevent mobile device intrusion. Based in San Francisco with an R&D center in Tel Aviv, Zimperium is calling its product zIPS, with an emphasis on IPS, which stands for intrusion prevention system. The app made to outwit attackers watches how a person's smartphone acts under normal conditions and it can identify what may be out-of-the-ordinary behavior.

Without reliance on signature detection, the app can find and prevent unknown threats, spear-phishing attempts (fraudulent email tricks), and network- and host-based attacks, according to the company. They said, "zIPS does not have to encounter any previously known kind of attack in order to protect your mobile device." What's more, "zIPS is capable of monitoring processes outside of its own sandbox, making it entirely dynamic and independent of signatures." What could look like a benign app could in time process to download mobile attack. Being "dynamic," zIPS can outwit the intruders. Rather than presenting the product for the consumer, though, Zimperium is targeting its product, for now, toward organizations that have the protection of BYOD security in mind. They will be leveraging this new chapter in business connectivity that reaches beyond desktop PCs into employees' tablets and smartphones used regularly for working at home and on the move.

Successful detection of malware on such mobile devices is not easy. "Regardless of your bring-your-own-device policy," said the team, "not even the very best antivirus programs can protect a device from infiltration if the carrier for instance unwittingly connects to the same WiFi network as a hacker, opens fake emails or downloads previously unknown (zero days) malware."

The company was founded in 2010 by CEO Zuk Avraham, who served in the IDF as a security researcher, and Elia Yehuda, a white-hat hacker.

A report from analysts Juniper Research, announced in November, forecast that the number of employee-owned smartphones and tablets used in the enterprise will exceed 1 billion by 2018. The report also indicated that the threat from unprotected employee mobile devices is of significant importance. In October, Juniper Research, had announced findings that more than 80 percent of the total enterprise and consumer-owned smartphone device base would remain unprotected through 2013, despite increasing awareness of mobile security products.

More information: www.zimperium.com/

Citation: BYOD mobile attack prevention app uses machine learning (2014, January 24) retrieved 4 May 2024 from https://techxplore.com/news/2014-01-byod-mobile-app-machine.html