Check Point Research has discovered a new variant of mobile malware that has quietly infected around 25 million devices, including 15 million mobile devices in India. Disguised as a Google-related application, the malware exploits known Android vulnerabilities and automatically replaces installed apps with malicious versions without users' knowledge or interaction.

Dubbed "Agent Smith", the malware currently uses its broad access to the devices' resources to show fraudulent ads for financial gain, but could easily be used for far more intrusive and harmful purposes such as banking credential theft and eavesdropping. This activity resembles previous malware campaigns such as Gooligan, Hummingbad and CopyCat.

Sharing details of the malware, Jonathan Shimonovich, head of mobile threat detection research at Check Point Software Technologies, said, "The malware attacks user-installed applications silently, making it challenging for common Android users to combat such threats on their own. Combining advanced threat prevention and threat intelligence while adopting a 'hygiene first' approach to safeguard digital assets is the best protection against invasive mobile malware attacks like 'Agent Smith'. In addition, users should only be downloading apps from trusted app stores to mitigate the risk of infection as third party app stores often lack the security measures required to block adware loaded apps."

Agent Smith was originally downloaded from the widely-used third party app store, 9Apps and targeted mostly Hindi, Arabic, Russian, Indonesian speaking users. So far, the primary victims are based in India though other Asian countries such as Pakistan and Bangladesh have also been impacted. There has also been a noticeable number of infected devices in the United Kingdom, Australia and the United States.

About Us   We are Hiring   Contact Us

Subscribe   Privacy Policy   Advertise   Terms & Conditions