Written by Marco Attard
06 November 2015

The Kaspersky Labs IT Threat Evolution Q3 2015 Report warns of increasing mobile malware, marking out an opportunity within the security industry.

The report compiles information gathered by "millions" of Kaspersky product users in 213 countries.

According to the report Kaspersky mobile security products detected 323374 new malicious mobile programs-- a 10.8% increase over Q2 2015 and a 3.1-fold increase since Q1 2015. Malicious packages installed on mobiles during the quarter total 1.5 million, 1.5 times more than Q2 2015.

The company says such programs are "very difficult" to fight, since they often root devices and use superuser privileges. As a result, Trojans account for over 50% of the most popular mobile malware.

"The number of programs displaying intrusive advertising on mobile devices (adware) continued to grow in Q3 and accounted for more than half of all detected mobile objects," the report reads. "We have also observed a growing number of programs that use advertising as the main monetisation method while also using other methods from the virus writers' arsenal."

Online banking is another risky segment-- Kaspersky solutions blocked around 626000 attempts at malware able to steal money via online banking access, -17.2% less than Q2 2015, if a 5.7% Y-o-Y increase. Q3 2015 notifications involving attempted malware infections to steal money from online banking systems total 5.68m.

Interestingly Austria leads in banking Trojan attacks, as 5% of Austrian Kaspersky customers faced such attacks during Q3 2015. Singapore (4.2%) and Turkey (3%) follow. The most prevalent means of attack beang Trojan-Downloader.Win32.Upatre, used in 63.1% of attempts at stealing user payment details.

Meanwhile the Kaspersky Lab Global Research and Analysis Team (GReAT) reports on sophisticated attack campaigns, including the Turla group (uses satellite communications to manage command-and-control server traffic), Darkhotel APT (infiltrates hotel wifi networks to place backdoors on target computers) and Blue Termite APT (focuses on stealing information from organisations in Japan). Kaspersky is also collaborating with the Dutch National High Tech Crime Unit (NHTCU) and Panda Security, leading to the arrest of 2 suspects believed to be involved in the CoinVault ransomware attacks.

“The developments in Q3 demonstrate that the global threat landscape is continuing to evolve at a fast pace. Malicious mobile programs are on the rise and in countries where online banking is popular, people are at considerable risk from Trojans looking to target them," GReAT says. "With 5.6m cases of attempted theft from online bank accounts, and cyber-criminals continually developing sophisticated attacks, the use of high quality cybersecurity products has never been more important. It’s vital that all those using the Internet-- both individuals and organisations-- protect themselves from these growing threats."

Go Kaspersky Labs IT Threat Evolution Q3 2015 Report