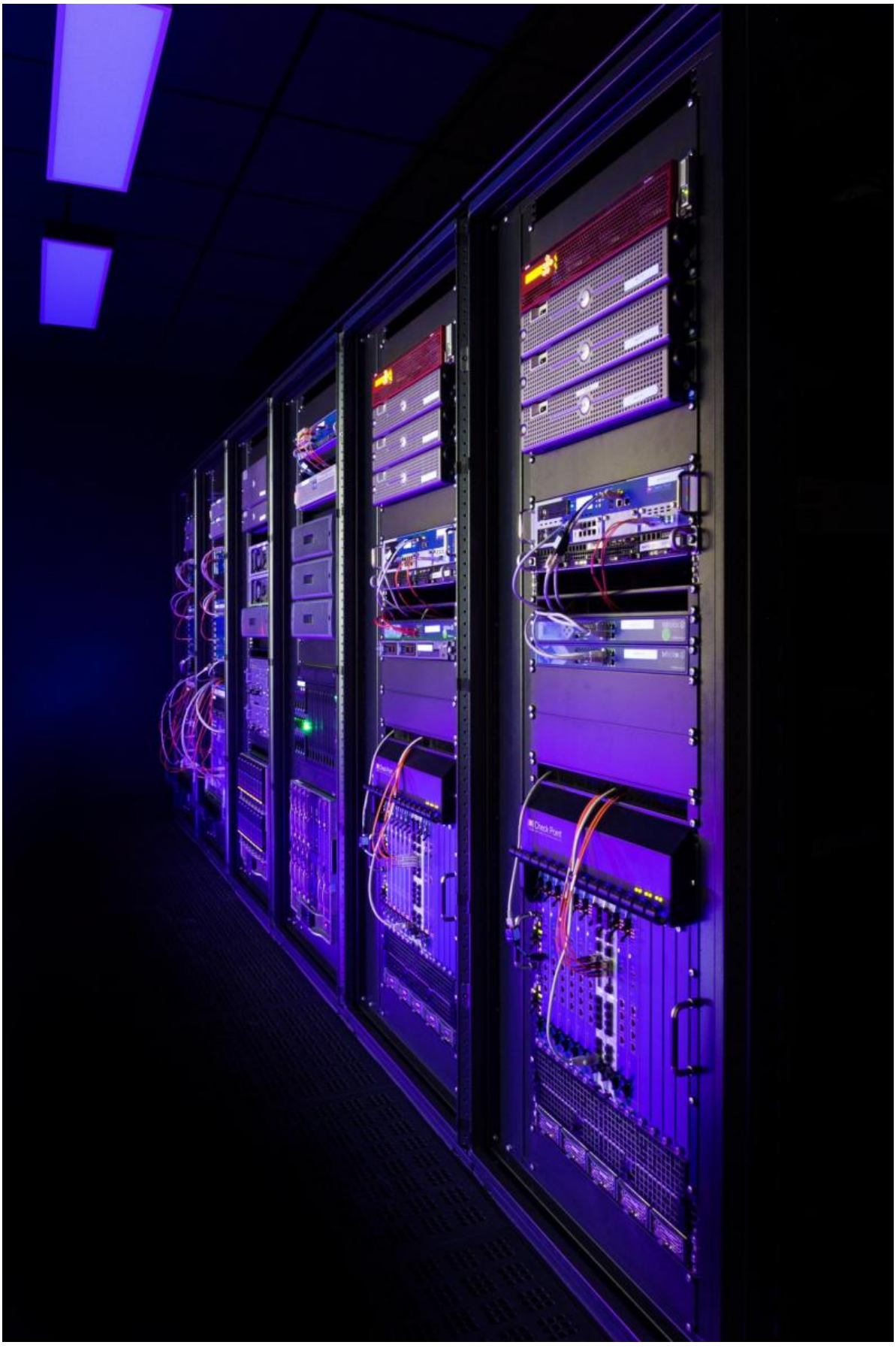
Nokia malware report shows smartphones now account for 60% of infections in the mobile network

March 2 2016



Nokia Security Center server room in Berlin

Nokia Security Center Berlin, powered by Nokia Threat Intelligence Lab, today released research findings showing that in the mobile networks, smartphones pulled ahead of Windows-based computers and laptops, now accounting for 60% of the malware activity observed in the mobile space. The Nokia Threat Intelligence Report also reveals an increase in iOS-based malware, growing sophistication of Android malware and the rising threat of mobile ransomware.

The report examines general trends and statistics for malware infections in devices connected through mobile and fixed networks. Data is aggregated where Nokia malware detection technology is deployed, with more than 100 million devices covered.

Nokia Threat Intelligence Report at a glance:

- Due to a decrease in adware activity, the overall infection rate in mobile networks declined from 0.75% to 0.49% on Windows-based PCs connected to the Internet via a mobile network in the second half of 2015. Adware is a software that automatically displays or downloads advertising material (often unwanted) when a user is online.
- In the same time period, smartphone infection rates increased and now account for 60% of infections detected in the mobile networks.
- Android continues to be the main mobile platform targeted
- For the first time since the report began, iOS-based malware – including XcodeGhost and FlexiSpy – is on the top 20 list. In

October 2015 alone, iPhone malware represented 6% of total infections.

- The XcodeGhost malware was injected into apps through a compromised software development kit that was used by Chinese developers to create legitimate apps distributed via the Apple App Store. Apple has removed these apps from the Apple Store, but some malware remains active.
- Ransomware - malware that effectively holds a device hostage by encrypting data and then locking it - like CryptoLocker has been around for a while on Windows PCs, but 2015 saw several varieties attacking Android, as well. Recovery can only be achieved by paying the attacker a ransom fee via a prepaid cash voucher or with bitcoins.
- Mobile malware is becoming more sophisticated in the techniques it uses to persist on the device. It is becoming very difficult to uninstall and can even survive a factory reset.

Kevin McNamee, head of the Nokia Threat Intelligence Lab, said: "Security is a very real concern for any device with an IP address, be it Android, iPhone or even a Windows PC connected to the mobile network. While Android infections continue to rise and become more sophisticated, the Nokia Threat Intelligence Report from late 2015 was the first time we saw iOS malware make our top 20 list, with XcodeGhost being the fourth most prevalent malware detected. We also saw a rise in a variety of ransomware apps that try to extort money by claiming to have encrypted the phone's data. Nokia's security approach reaches into the network to stop malware before getting to the device itself and before damage can occur."

Did you know?

The modern smartphone presents the perfect platform for corporate and personal espionage, information theft, denial of service attacks on

businesses and governments, and banking and advertising scams. It can be used simply as a tool to photograph, film, record audio, scan networks and immediately transmit results to a safe site for analysis.

More information: Click here to download the full report, including malware list and methodologies: resources.alcatel-lucent.com/asset/193174

Provided by Nokia