RiskIQ uncovers ‘app attack’ threat to high street brands

Contributed by RiskIQ
Tuesday, 16 June 2015

New research from RiskIQ, the Digital Footprint Security company, highlights the risks posed to UK organisationâ€™s and their customers from unauthorised or fraudulent mobile apps and unauthorised app stores. Companies spanning retailers, travel companies, media & entertainment, gambling firms and banks have far more mobile apps owned by them or referencing their brand than they are aware of, many of which come from a new breed of hacker intent on compromising their digital assets and putting their customers at risk.
The research found that, on average, nine-in-ten apps exist in un-official stores, places brands are unaware of which is leaving brand assets vulnerable to compromise. With hundreds of mobile app stores and more than 11 million apps now being marketed, the ability to police and protect digital assets is becoming harder to achieve.

Apps that are not genuine place the consumer at a disadvantage. At the best they can lead to a poor brand experience, which reflects badly on the business; at the worst, malicious apps can compromise a usersâ€™ security and lead to the spread of malicious viruses. The study by RiskIQ examined the mobile footprint of 45 top UK companies across five vertical sectors, to give a snapshot of the vulnerabilities they face.

In addition, RiskIQ discovered 31,078 brand-associated apps had been blacklisted out of a total of 186,655, (17% of the total), or the equivalent of 690 per company. Blacklisting occurs when an app fails a virus scan by one or more of the major virus vendors or if it links to a URL or IP address that is a known source of malware.

The study also found 6,377 feral apps (3.4% of the total), mobile apps that are hosted on a web site and not in a store, making them even more difficult for companies to find and take down.

Ben Harknett, RiskIQ Managing Director EMEA, says: â€œAs a consumer, mobile apps are all about keeping us entertained and making it easier for us to interact with the brands we love. As a business this customer dependency on apps means ensuring a good customer experience is crucial. Not only do organisations have to ensure that the apps are thoroughly tested from a functionality, performance and security perspective, but that once released are monitored to ensure the customer is getting the experience they expect.

â€œThis is more difficult than you might expect. While Google Play, iTunes, and Windows Phone capture a large part of the market, there are hundreds of other app stores competing to drive traffic and capture a share of the worldwide mobile app market. Hackers are increasingly leveraging mobile as a new attack vector, especially the Android platform, which is one of the most popular platforms worldwide. But its attraction is also a drawback as it doesnâ€™t require users to jailbreak or root devices in order to install apps from unverified sources.â€•

In the modern mobile environment thereâ€™s an app for everything. The constant demand for more apps has been driving a growth not just in the number of apps available on the market but also the number of app stores hosting them. RiskIQâ€™s research revealed that on average, applications featuring a company brand were found in 56 different app stores. In total, companies each have 4,148 mobile applications attributed to their brand.

Unsurprisingly, the gambling sector had the highest problem with unauthorised apps â€“ with 12,742 apps per brand and the highest number of blacklisted apps â€“ on average 2,306 per company. In contrast, the Retail Banking sector appears to have tighter control of their application footprint with only 5,288 applications in un-authorised app stores. They also had the lowest number of blacklisted apps, with a total of 60 across the sector.

Gambling companies also had the highest number of feral apps, averaging 446 per company, whilst retail banking had the fewest at 10 per company.

â€œA blacklisted application can be detrimental to an organisation; many of these applications will contain malicious capabilities to do everything from treat a device as a form of revenue generation using click fraud through to monitoring an individual users movements by accessing geo-location capabilities in a device and replicating data. For the brands associated with these applications the need to remove them from circulation is vital as customers will place the fault of the malware with the brand and not the rogue application,â€• said Harknett.

â€œAt RiskIQ we work with organisations all over the globe to uncover just how many mobile applications are associated with their brand, helping them tackle the malware problems they face so that they can continue to deliver an excellent level of service to their customers,â€• Harknett concluded.