App Economy under Attack: Report Reveals More than 90 Percent of the Top 100 Mobile Apps Have Been Hacked

SAN FRANCISCO, August 20, 2012 — Ninety-two percent of the Top 100 paid Apple iOS apps and 100 percent of Top 100 paid Android apps have been hacked, according to new research contained in the *State of Security in the App Economy: Mobile Apps under Attack* report. The report, which reveals the widespread prevalence of "cracked" mobile apps and the financial impact befalling the multi-billion dollar App Economy due to compromised brands, lost revenues, intellectual property (IP) theft, and piracy, was released today by Arxan Technologies.

The proliferation of mobile devices has created an app-centric global marketplace, ushering in the App Economy that is driving new business models and revenue streams across all industries. In its *State of Security in the App Economy* report, Arxan set out to analyze the extent of malicious mobile app hacking by researching hacked versions of top Apple iOS and Android apps from third-party sites outside of the Apple App Store and Google Play marketplaces. The sample of 230 top apps included the top 100 paid Apple iOS and top 100 paid Android apps as well as 15 highly popular free apps for iOS and the same 15 free apps for Android.

Key findings of the report reveal:

- **More than 90% of top 100 paid mobile apps have been hacked:** 92% of top paid iOS apps and 100% of top paid Android apps were found to have been hacked.
- **Free apps are not immune from hackers:** 40% of popular free iOS apps and 80 percent of the same Android apps were found to have been hacked.
- **Hacking is pervasive across all categories of mobile apps:** Hacked versions of mobile apps were found across all key industries such as games, business, productivity, financial services, social networking, entertainment, communication, and healthcare.
- **Mobile apps are subject to many diverse types of hacks and tampering attacks**, such as disabled or circumvented security, unlocked or modified features, free pirated copies, ad-removed versions, source code/IP theft, and illegal malware-infested versions.
- **The *Anatomy of an App Hack* entails three steps:** Define the exploit and attack targets; reverse-engineer the code; and tamper with the code; this process is made easy with widely available free or low-cost hacking tools.
- **Financial risks from hacking are increasing rapidly:** Mobile app hacking is becoming a major economic issue with consumer and enterprise mobile app revenues growing to more than $6o billion by 2016 and mobile payments volume exceeding $1 trillion (based on data from KPMG, ABI Research, and TechNavio).

A copy of the complete *State of Security in the App Economy: Mobile Apps under Attack* report can be accessed at:http://www.arxan.com/resources/state-of-security-in-the-app-economy/

"We envision a thriving App Economy with freedom and confidence to innovate and distribute new apps. However, this potential is being threatened by hackers, and most enterprises, security teams, and app developers are not prepared for these attacks," said Jukka Alanen, vice president at Arxan and the lead author of the new study. "The integrity of mobile apps can be easily compromised through new tampering/reverse-engineering attack vectors. The traditional approaches to application security such as secure software development practices and vulnerability scanning cannot address the new hacking patterns that we identified. The findings call for new approaches for mobile app owners to build protections directly inside their apps to withstand these new attacks."

"As consumer devices such as iPhones and iPads proliferate in the enterprise and among consumers, the number of organizations interested in custom development of mobile applications is steadily on the rise. We've already seen mobile apps take off in the financial sector, with online banking, check cashing, and online trading apps. Security, although a prime driver for custom development, is one of the hardest aspects to get right," wrote Chenxi Wang, Ph.D., vice president and principal analyst at Forrester Research, Inc., in the June 2011 research report, *Building Secure iPhone and iPad Apps***.**

The State of Security in the App Economy report also offers a look into the tactics employed by hackers, enabling application developers and security teams to better understand the methods used which threaten the emerging App Economy. Additionally, the report suggests organizations leverage mobile app protection to enable them to freely innovate and distribute high-value and sensitive mobile apps with confidence.

Specific recommendations outlined in the report include:

- **Make mobile app protection a strategic priority**, reflecting its new criticality to address hacking attacks and the growing value at stake.
- **Be especially diligent about protecting mobile apps that deal with transactions, payments, sensitive data, or that have high-value IP** (e.g., financial services, commerce, digital media, gaming, healthcare, government, corporate apps).
- **Do not assume that web app security strategies are adequate** to address the new requirements for mobile app protection.
- **Focus app security initiatives on protecting the integrity of mobile apps against tampering/reverse-engineering attacks, in addition to traditional approaches to avoiding vulnerabilities.**
- **Build protections directly into the app** -- harden the code against reverse-engineering, and make the app tamper-proof and self-defending -- to counter how hackers attack an app.