ESPION WHITE PAPER DELIVERS SECURITY WARNING TO BUSINESSES LAUNCHING APPS

Submitted by: Espion Group
Thursday, 8 November 2012

AVOIDING APP APOCALYPSE

Leading information security firm Espion, with locations in Manchester, Edinburgh, Dublin and Brussels, is spearheading safe app development by urging businesses to make security a top priority when bringing apps to the marketplace.

To support this, Espion has launched a new white paper titled: ‘Securing Mobile Applications’ a best practice guide to making apps safe which outlines the significant risks posed by insecure apps with the potential to unleash financial and reputational damage on businesses.

In recent months, thanks to new tools as well as reduced barriers to entry, app development has become faster and cheaper to execute. Businesses that fail to apply secure robust testing in app design and development risk launching a product that is easy for criminals to exploit for malicious gain or is vulnerable to confidential customer data being leaked or transmitted.

Top of the ways criminals are exploiting flawed apps identified in Espion’s white paper centres on ‘Activity Monitoring and Data Retrieval’. Here criminals track and intercept the victim’s sensitive information by either listening in to their phone calls or watching as they send emails from a mobile. Another cause for concern is ‘User Interface Impersonation’ where a malicious app is unknowingly downloaded instead of a legitimate version or where various malicious UI facades are used. The doppelganger retrieves and sends the attacker the victim’s sensitive information such as online banking login details. Another costly scam is ‘Unauthorised dialing, SMS and payments’ which involves hijacking the victim’s phone with a Trojan app allowing premium rate phone calls and SMS messages to be made.

Espion also outlines other scenarios facing businesses with inadequate app security including: loss of confidential data; disclosure of credentials; privacy violations and breach of compliance. This is because insecure mobile apps can leak device information thus exposing it to third parties or can store sensitive information, in an unencrypted or cache format, making it easier to be compromised.

Mobile app security expert, and senior consultant at Espion, Darren Fitzpatrick says: “With the mobile applications boom in full swing we are urging businesses not to take security shortcuts in the race to use this technology to engage with their customers. Organisations need to realise the onus is on them to apply due diligence to safeguard their app users from serious breaches of privacy and/or criminal violation.

Whether an app is developed in-house or by a third party, by failing to include robust security testing in the development process they are negating their compliance obligations.”

For IT professionals tasked with launching apps, ‘Securing Mobile Applications’ is an invaluable resource and a unique opportunity to take advantage of Espion’s unrivalled, specialist expertise around

effective development and secure deployment. The best practice guidelines in the white paper will enable organisations to mitigate the risks of security breaches as well as meet their governance and compliance obligations.

Espion's white paper 'Securing Mobile Applications' is free to download at http://www.espiongroup.com/security-management.

-ends-

Notes to the editor

REASON WHY APPS ARE MORE VULNERABLE THAN COMPUTERS:
Unlike traditional computing environments mobile devices rely exclusively on wireless-based communication, are highly connected to web services, have more direct payment capability, are more likely to be lost or stolen and interact with sensors from devices such as microphones, cameras, location detectors etc. What's more, they are often consumer-owned, yet are often used to access corporate email and other parts of an organisation's internal network. All of these factors have has spurned new opportunities for criminals to exploit.

KEY "MALICIOUS FUNCTIONALITY" RISKS INCLUDE:
• Activity Monitoring and Data Retrieval: this involves the real time interception of data as it is being generated on the device - e.g. sending emails from the device to hidden third party addresses, open microphone recording, letting attackers listen in on phone calls, relaying of contact information and so on
• Unauthorised dialing, SMS and payments: this involves criminals injecting premium dialling functionality via Trojan mobile apps and getting mobile carriers to collect and distribute money to them
• Unauthorised network connectivity (exfiltration or command & control): this involves use of a range of potential vectors to send data to the attacker, or direct commands or actions to spyware. Channels include email, SMS, HTTP GET/POST, TCP or UDP sockets, DNS, Bluetooth or Blackberry messenger channels.
• UI Impersonation: In the mobile app context this may involve links between an app and a native web site - taking the online banking example, the app may still function normally between the mobile app UI and the native web app, but would unknowingly act via a proxy that skims sensitive details for malicious use at a later stage. This may be caused by a malicious app being unknowingly downloaded instead of a legitimate version, analogous to how a phishing attack occurs in a pure web scenario.
• System modification: this is where mobile system configuration details are modified to gain privileged access to the device - for example modifying the Access Port Name at the network device OS level, allowing malicious rerouting of traffic between data networks and the internet.

KEY "VULNERABILITY" RISKS INCLUDE:
• Sensitive data leakage: insecure mobile apps can leak device information, authentication credentials, exposing it to third parties
• Unsafe sensitive data storage: applications may store sensitive information in unencrypted form or may cache data in a way that can be compromised. This can result in loss of confidential data, disclosure of credentials, privacy violations and potential non-compliance
• Unsafe sensitive data transmission: Similarly, applications may transmit data wirelessly in an

insecure manner – use of SSL can alleviate this, provided that the app does not degrade from HTTPS to HTTP, and handles invalid certificates correctly
• Hardcoded password/keys: application developers hardcode passwords in applications as a debugging shortcut or to make it easier to implement – this makes the password recoverable via reverse engineering.

The white paper references both Veracode (www.veracode.com) and OWASP (Open Web Application Security Project - www.owasp.org) priority lists of mobile application risks as well as Espion's original mobile app testing framework and how it can support effective development and secure deployment of your applications.

ABOUT ESPION:
Espion is an award-winning information security firm with dedicated specialist areas in Information Governance, Security Management, Forensics & eDiscovery, Research, Training and Technology Distribution.

For more than a decade, Espion has been committed to helping market leading companies from all sectors solve critical information security issues by providing strategic advice and solutions for the holistic Compliance, Protection and Management of their most valuable asset – information.

What sets us apart is our genuine depth and breadth of expertise which spans the entire spectrum of information security combined with in-depth knowledge of leading technologies and adherence to industry best practices.

Espion boasts being one of the Deloitte Technology Fast 50 for five years in a row in recognition for continually creating effective responses to new developments in the field of information security.

FOR MORE INFORMATION ON ESPION PLEASE CONTACT:

Isabel Dalton
m: +353 87 2639021
t: +353 1 2101711
Isabel.dalton@espiongroup.com