MWR InfoSecurity to release drozer at Black Hat Arsenal in Las Vegas, USA, on August 1st.

Wednesday 24 July, 2013

Companies using Android mobile devices can now safeguard their assets and IT infrastructure by using drozer, the new Android security testing framework, to run full security assessments.

Previously known as Mercury, drozer allows for dynamic analysis of applications running on Android devices. The tool now has a new set of features that include the ability to compromise Android devices through publicly available exploits. These features are designed to help an organisation understand how a technical vulnerability on a mobile device can become a real threat to their business.

“We added a number of aspects to drozer that weren’t included in Mercury, but the major new feature consists of a means of getting the application onto an Android device remotely. Traditionally, it had to be downloaded from the marketplace or installed using the developer features,” said Daniel Bradberry, Head of Security Tools Development at MWR InfoSecurity.

Tyrone Erasmus, Senior Security Consultant at MWR InfoSecurity, said: “It is a major step forward as previously, various remote Android exploits were scattered across the internet and in some cases were not very reliable. Taking up Mercury’s lead, drozer unifies these publicly available exploits into a single framework and improves the quality of the exploitation code and payloads available to the penetration tester.”

He added: “This opens the opportunity of embracing company smartphones and other Android devices when performing a full security assessment of an organisation’s IT network, which is particularly important at times when companies are introducing BYOD (Bring Your Own Devices) strategies and taking up consumer devices for corporate use.”

Android developers and security researchers will now be able to exploit vulnerabilities in Android’s operating system and use them to install the application on the phone remotely, such as using a malicious document to deploy the app ‘without the user noticing it’.

For example, security consultants employed by an organisation can use drozer in a red team exercise, where they have an open scope to attack assets belonging to a company to test its digital infrastructure and security standards. The tool will now allow them to expand the attack surface to include mobile devices as a path of entry into a company’s network.

The team from MWR Labs, the company’s research arm, has successfully tested drozer and was able to gain access to personal information and pictures on Android devices, take screenshots and record from the microphone.

Tyrone Erasmus said: “By incorporating publicly available exploits into drozer, we enable businesses to simulate attacks against mobile devices in their network. For instance, by gaining access through a security breach in the user’s mobile web browser, we are able to install the tool on the device and use it to help them understand how their business and entire IT infrastructure could be exposed to an attacker.”

Daniel Bradberry added: “The development of drozer has been driven by substantial feedback from the community. Mercury had security assessment and post-exploitation neatly covered off but lacked the capability of being installed remotely on a device through exploitation. This is why we decided to add this new feature and change the name to drozer.”

Similar to Mercury, drozer provides support for any Android device running Android 2.1 and all later versions, covering 99% of the devices in the market. It is an open-source tool and will be available to download from the MWR Labs website - http://mwr.to/drozer - immediately after being presented at Black Hat USA.

Daniel Bradberry and Tyrone Erasmus will be tweeting useful hints and tips from @mwrdrozer.

-Ends-

Press Contact:
Julian Menendez

Related Sectors:

Business & Finance :: Consumer Technology ::

Related Keywords:

MWR InfoSecurity :: Drozer ::

Scan Me:

T: +44(0)20 7544 8831?
E: julian@barzilay.co.uk ?

Note to editors:
MWR's Black Hat Arsenal presentation on August 1st will include:
How to remotely gain access to Android devices using drozer
Some of the innovations that MWR has come up with regards to Android exploitation payloads
How to integrate new remote exploits into the framework
A variety of exploitation examples exposing sensitive data from a compromised Android device
Black Hat remains the best and biggest event of its kind, providing a series of highly technical information security conferences that bring together thought leaders from all facets of the infosec world. Black Hat focuses on the sharing of practical insights and timely, actionable knowledge.

drozer - Powerful penetrative Android security testing
drozer allows developers and testers to assume the role of an app and to execute test case code by running an Agent on the Android device, which is connected to a Console on their PC. These code modules, which interact with the Dalvik VM and the underlying operating system, are easy to write, reuse and share.
drozer lets testers build malicious webpages and perform drive-by downloads of a drozer Agent onto visiting devices, or create malicious files that exploit a parser to install an Agent onto the devices that open it. Depending on the permissions granted to the application it exploits, drozer can install a full agent or inject a limited agent into a running process, to act as a Remote Access Tool (RAT).

About MWR InfoSecurity
MWR InfoSecurity is one of the world's leading information security consultancies - MWR specialises in identifying, managing and mitigating Information Security risks.

The company undertakes simulated cyber attacks with organisations across different industries to help them understand the security threats they are facing.??

visit http://www.mwrinfosecurity.com/?

Company Contact:

_

Rocket Pop PR

E. rocketpoppr@outlook.com

Additional Contact(s):
Jean Matthews
Samantha Jones

Beehive Mill
Jersey Street
Manchester
M4 6AY

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.rocket-pop-pr.pressat.co.uk