Prey Inc. Refutes Election Malware Claims of Malaysian PKR

Affirms Prey Anti-Theft is not capable of tampering with voting process

San Francisco, November 12, 2018 – Prey Inc., provider of the cross-platform, open-source anti-theft software that protects more than eight million mobile devices, addresses today recent accusations against Prey' software by PKR deputy presidential candidate Rafizi Ramli and JPP chairman Datuk Rashid Din during the PKR elections in Malaysia, in which the results in the Julau district of Sarawak of said elections were suspended due to a supposed security breach in a set of tablets utilized as e-voting machines. Prey affirms that its Prey Anti-Theft software is not capable of carrying out the specific election tampering activities.

For more than seven years, the open-source Prey Anti-theft application has enjoyed worldwide acceptance for its ability to protect phones, tablets, and laptops against theft and their data against loss. As a company, Prey Inc. also provides Enterprise solutions for recognized companies, universities, and non-governmental organizations globally.

In this alleged breach, the Prey Anti-theft mobile app was found installed, allegedly without authorization. It is still being debated if the application was installed by party election workers looking to secure the devices, since installing applications required Administrator credentials, or if was installed by third-party individuals looking to tamper or disrupt the devices.

In these recent allegations, Prey's software has been incorrectly accused of:

- Eliminating voting applications installed on the tablets
- Manipulating voting decisions remotely
- Wiping out votes on the tablet, as a feature
- Controlling the tablets remotely as a remote desktop
- Being a malware and spyware application
- Breaching password-protected systems to install the application

Prey Inc. confirms that its software is not capable of carrying out said activities, being that the application itself has no Remote Desktop feature, and no remote control capabilities that allow the deletion of specific applications or the ability to write or modify data in the device.

Prey's free features include device tracking and security actions such as the remote screen lock, the alarm, and message alert. The Remote File Retrieval and Remote Wipe features are part of paid plans exclusively; furthermore, Remote Wipe is only capable of wiping the SD card or to format the Android device completely. It cannot target files specifically or modify them to alter their content.

Prey Inc. also discredits allegations that describe Prey as malware capable of bypassing in-device security that avoids unauthorized user modifications, such as tampering of data or installing applications. When said protections are active, the application can only be installed by the device's Administrator.

The company was not, at any given moment, involved in the election process or in the configuration of the devices utilized; moreover, Prey Inc. isn't responsible for the organization or disruption of the security measures that are to be taken to protect e-voting devices during events of such sensibility.

Prey is committed to the protection of our users privacy and security. We have complied with the GDPR regulation since it came into effect, so that users can be protected by the highest worldwide privacy standards. Even if the European regulation is bound specifically to all activities inside that continent, Prey Inc. applies these terms and standards globally to ensure all users around the globe are covered. We have also kept our software as an open-source, due to established trust between our solution and the community.

We believe the candidate's words come in good faith and stem from a misunderstanding of how the software works. Given this position, we refrain for now to pursue further legal actions.

About Prey Inc.
Prey Inc. is is the only provider of anti-theft solutions for tracking and protecting mobile devices that can manage and secure all of an organization's mobile devices from the same place. Installed on more than 8 million devices worldwide, Prey's cross-platform, open-source security solution consolidates mobile device management on a single account, no matter how many different device manufacturers or operating system need to be tracked. Find out more at www.preyproject.com

Media Contact
Mike Schultz | Cavalier Communications
Phone: 978-496-1012
Mike@cavalier-communications.com