Fighting the rise of the app attackers

February 26 2014

Researchers have been given a share of £3 million by the Engineering and Physical Sciences Research Council (EPSRC) to counter cyber-criminals who are using malicious apps which can collude with each other to infect the smartphone in your pocket.

Malware attacks are rising year on year – and over one million new Android malware attacks were identified in 2013 by McAfee, a division of Intel Security.

Malicious apps can gain access to address books, GPS coordinates, passwords or pin numbers. They can redirect your data across the net, send you to phishing sites and also bypass the two-step authentication process used to access an ever-increasing number of online services such as banking or email. Criminals can monetise this information in a number of ways – by getting your phone to send messages to premium numbers, by remotely controlling an infected phone, by tricking you into revealing passwords and by using your stolen data.

The £3 million is funding two app research teams at Royal Holloway University of London, and City University London, Coventry and Swansea Universities as well as three teams carrying out research to enhance the UK's cyber-security.

Dr Lorenzo Cavallaro, Lecturer in the Information Security Group at Royal Holloway University of London, said: "You may think that the phone in your pocket is safe, but think again. We're used to considering our phones as a trusted, private channel of communication, and suitable to receive authentication information to access specific online services. Unfortunately, this information can be leaked or abused by colluding malware if the mobile device is infected."

Dr Cavallaro's research team will study the behaviour of apps on Android operating systems and develop novel techniques to spot malicious apps, which of course, are designed to remain hidden. They will use this information to enrich or enhance devices to counteract attacks.

The latest cyber-threat to smartphones comes from apps working together or colluding. An example of collusion consists of one app permitted to access personal data, which passes the data to a second app allowed to transmit data over the network. This information can then be used by criminals.

Professor Tom Chen is leading research teams at City University London, Swansea and Coventry universities on app collusion detection. He said: "Currently almost all academic and industry efforts are focusing on single malicious apps; almost no attention has been given to colluding apps. Existing antivirus products are not designed to detect collusion."

The team will develop new techniques to detect colluding apps and will curtail the threat before it becomes widespread. By design, Android is "open" in its flexibility to download apps from different sources. Its security depends on restricting apps by combining digital signatures, sandboxing, and permissions. These restrictions can be bypassed without the user noticing by colluding apps whose combined permissions allow them to carry out attacks that neither app could carry out alone.

Both research teams are partnering with McAfee, a division of Intel Security. The security company is providing researchers access to a library of safe apps and will assist in analysing malware so the researchers can test their behaviours.

Dr Igor Muttik, a Senior Principal Architect at McAfee, a division of Intel Security said: "We're up against really sophisticated malware - some even used by nation states for spying. All attackers are well aware of the technology involved in detecting and tracking them. These cybercriminals often take an industrial approach to malware; they try to maximise their benefits from it. So, we need to constantly raise the bar by improving the technology and this will make it more complex and less profitable for them to operate."

Professor Chen, City University London, has some advice for smartphone users: "Be careful which apps you download, particularly if downloading from an unofficial app store, and be wary of an app which asks you to grant lots of permissions before it is installed."

Provided by Engineering and Physical Sciences Research Council

Citation: Fighting the rise of the app attackers (2014, February 26) retrieved 3 April 2024 from https://phys.org/news/2014-02-app.html