FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

Same weakness found in 7 cloud storage services

PRESS RELEASE
25.June 2012

Cloud storage services allow registration using false e-mail addresses – Fraunhofer SIT sees the possibility for espionage and malware distribution.

Security experts at the Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt have discovered that numerous cloud storage service providers do not check the e-mail addresses provided during the registration process. This fact in combination with functions provided by these service providers, such as file sharing or integrated notifications, result in various possibilities for attacks. For example, attackers can bring malware into circulation or spy out confidential data. As one of the supporters of the Center for Advanced Security Research Darmstadt (CASED), the Fraunhofer SIT scrutinized various cloud storage services. The testers discovered the same weakness with the free service offerings from CloudMe, Dropbox, HiDrive, IDrive, SugarSync, Syncplicity and Wuala. Scientists from Fraunhofer SIT presented their findings on the possible forms of attacks on June 26, 2012, at the 11th International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom) in Liverpool.

Attackers do not require any programming knowledge whatsoever to exploit these weaknesses. All they need is to create an account using a false e-mail account. The attacker can then bring malware into circulation using another person’s identity. With the services provided by Dropbox, IDrive, SugarSync, Syncplicity and Wuala, attackers can even spy on unsuspecting computer users with the help of the false e-mail address by encouraging them to upload confidential data to the cloud for joint access.

Fraunhofer SIT informed the affected service providers many months ago. And although these weaknesses can be removed with very simple and well-known methods, such as sending an e-mail with an activation link, not all of them are convinced that there is a need for action. Dr. Markus Schneider, Deputy Director of Fraunhofer SIT: “Dropbox, HiDrive, SugarSync, Syncplicity and Wuala have reacted after receiving our information.” Some of these providers are now using confirmation e-mails to avoid this weakness, a method that has been in use for quite some time now. Others have implemented other mechanisms. “We think it is important that users are informed about the existing problems”, said Schneider. “Unfortunately, it is not possible to provide 100% protection against attacks, even if the affected services are avoided. It is therefore important that cloud storage services providers remove such weaknesses, as this helps to protect users more effectively.”

Consumers who use the affected services should be careful. Those who receive a request to download data from the cloud or upload data to it should send an e-mail to the supposed requestor to verify whether the request was really sent by them.