New malware could steal users social media behavior and info: researchers

October 14 2010

A new study by Ben-Gurion University of the Negev (BGU) researchers predicts that a new generation of malware (software written for malicious purposes like identity theft) could steal data on human behavior patterns, which is more dangerous than traditional, detectable attacks.

In the newly published paper, "Stealing Reality," Dr. Yaniv Altschuler and Dr. Yuval Elovici from BGU discuss malware threats that extract personal information about relationships in a real-world social network, as well as characteristic information about individuals in the network. Using mathematical models, based on actual mobile network data, the researchers demonstrated that malware attacks could be adapted to follow human behavior on social networks.

According to the researchers, "Many social networks collect important user data such as age, occupation and role, personality and more to create a 'rich identity.' With access to such sensitive information, the possibility for significantly more targeted and dangerous attacks is now open. There is a level of trust generated among users connected via social networks and these new threats, unbeknownst to the user, seek to violate it."

The research showed that in many cases a "stealth attack" (one that is hard to detect and steals private information at a slow pace) can result in the maximal amount of overall knowledge captured by the operator of this attack. This attack strategy also makes sense when compared to the natural human social interaction and communication patterns. The rate of human communication and evolution of a relationship is very slow compared to traditional malware attack message rates.

A "Stealing Reality" type of attack, which is targeted at learning the social communication patterns, could "piggyback" on the user-generated messages, or imitate their natural patterns, thus not drawing attention to itself, while still achieving its target goals.

One of the biggest risks of real world social media network information being stolen is that this type is very static, especially when compared to traditional targets of malicious attacks. For example, passwords, usernames and credit cards can be changed. An infected computer could be wiped and re-installed. An online e-mail, instant messenger or social networking account could be easily replaced with a similar one, and the users' contacts can be quickly warned of the original account's breach.

However, it is much harder to change one's network of real world, person-to-person relationships, friendships or family ties. The victim of a "behavioral pattern" theft cannot easily change his or her behavior and life patterns. Plus this type of information, once out, would be very hard to contain. In addition, once the information has been extracted in digital form, it would be quite hard, if not impossible, to make sure that all copies have been deleted.

The researchers explain in the study published on the arXiv.org website that "Many commercial entities have realized the value of information derived from communication and other behavioral data for a great deal of applications, like marketing campaigns, customer retention and security screenings. There is no reason to think that developers of malicious applications will not implement the same methods and algorithms into future malware, or that they have not already started doing so. There already exist secondary markets for resale of this type of information."

Provided by American Associates, Ben-Gurion University of the Negev

Citation: New malware could steal users social media behavior and info: researchers (2010, October 14) retrieved 25 April 2024 from https://phys.org/news/2010-10-malware-users-social-media-behavior.html