Abstract

Automated Social Engineering (ASE) is how social networking sites (SNSs) are exploited for Social Engineering by automated bots. Classical social engineering is an attack on the security of systems, based on exploiting human factors. ASE is an automated form of traditional social engineering which makes use of bots to attack SNS. One such bot is KOOBFACE [1] that infected Facebook for a long time until it was detected in mid of 2011 by Sophos lab. ASE bots can be developed easily using open source web automation and web scraping tools. These tools combined with appropriate chat logic with enhanced intelligence pose a great threat to the security of SNSs. Countermeasures like Captchas have proved ineffective in preventing bots from infiltrating SNSs. New techniques like Multi Modal Captchas (MMC), and Fast Flux Network (FFN) detection are the future of the ASE prevention. In this paper we present a survey of vulnerabilities, threats and propose some countermeasures for Automated Social Engineering.

References

- Jonell Baltazar, Joey Costoya, and Ryan Flores, "The real face of KOOBFACE:"
The largest Web 2.0 botnet explained, Trend Micro Threat Research, unpublished.
- M. Huber, "Towards automating social engineering using social networking sites" theses work 2009.

Index Terms

Computer Science
Information Systems

Keywords
Social Networking Sites (SNSs)   Fast-Flux Networks (FFNs)   Multi-Modal Captcha (MMC)
Automated Social Engineering (ASE)

botnet