

Experimental Analysis of Tools Used for Doxing and Proposed New Transforms to Help Organizations Protect against Doxing Attacks

Authors : Parul Khanna, Pavol Zavarsky, Dale Lindskog

Abstract : Doxing is a term derived from documents, and hence consists of collecting information on an organization or individual through social media websites, search engines, password cracking methods, social engineering tools and other sources of publicly displayed information. The main purpose of doxing attacks is to threaten, embarrass, harass and humiliate the organization or individual. Various tools are used to perform doxing. Tools such as Maltego visualize organization's architecture which helps in determining weak links within the organization. This paper discusses limitations of Maltego Chlorine CE 3.6.0 and suggests measures as to how organizations can use these tools to protect themselves from doxing attacks.

Keywords : advanced persistent threat, FOCA, OSINT, PII

Conference Title : ICCTICF 2016 : International Conference on Cyber Threat Intelligence and Cybercrime Forensics

Conference Location : Vancouver, Canada

Conference Dates : August 04-05, 2016