Memory forensics of Qakbot

By Borg, Steve (2020)

Title:	Memory forensics of Qakbot
Authors:	
Keywords:	Malware (Computer software) Computer security Digital forensic science
Issue Date:	2020
Citation:	Borg, S. (2020). Memory forensics of Qakbot (Bachelor's dissertation).
Abstract:	As malware is continuously evolving, a common technique used by malware authors is process injection, whereby malicious code is injected into benign processes with escalated privileges. In the past, signature-based detection may have been considered as a sufficient approach to malware detection. However, with the advent of polymorphism becoming one of the most prevalent detection evasion techniques, antivirus signatures are no longer effective due to malware’s ability to change its appearance at will. Qakbot malware is a prime example where despite several signatures have been written throughout the years, it has still managed to evolve and evade detection. Therefore, one would most likely have a late detection of the Qakbot Sample, making the use of digital investigation tools central for Incident Response. This malware has evolved and managed to blend into regular Windows processes, emphasising the importance of Memory Forensics to identify the exact workings of Qakbot and be able to reconstruct the timeline of events that occurred since the malware infection. A prominent obstacle to the analysis of the Qakbot malware is that it includes a packing layer, where parts of the malware are compressed to avoid detection and hinder analysis. In this dissertation, Reverse Software Engineering (RSE) and Dynamic Binary Instrumentation (DBI) techniques were used to produce forensic tools that will aid Incident Responders to identify exactly which processes are being created and potentially injected. The first two tools

	that were developed are based on state-ofthe- art system logs and memory forensics. The third and final tool that was developed, is a custom tool based on DBI and which through partial but timely memory dumps manages to get to that elusive infection evidence. The complete mobsync.exe misuse picture comes at the expense of computer memory and storage overheads.
Description:	B.Sc. IT (Hons)(Melit.)
URI:	https://www.um.edu.mt/library/oar/handle/123456789/76802
Appears in Collections:	Dissertations - FacICT - 2020 Dissertations - FacICTCIS - 2020

Files in This Item:

File	Description	Size	Format	
20BITSD002.pdf *Restricted Access*		2.02 MB	Adobe PDF	View/Open Request a copy