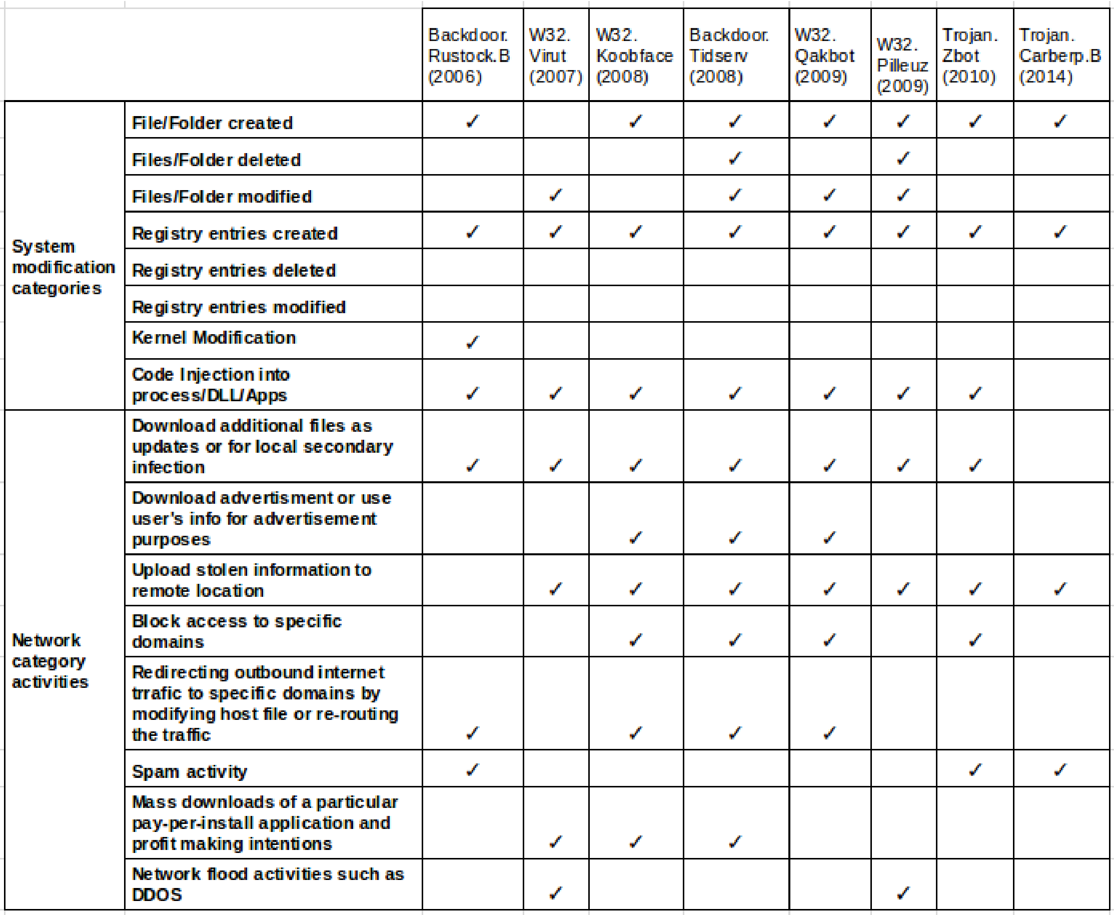
Comparision of malware functionalities intended for botnet formation

Mohammad Reza Memarian

December 18, 2014

In Figure 1, 8 malware's functionalities that were intended for botnet formation are compared. The comparison is done based on modifications that are made to the victim's system by the malware and network activitis of the zombies. The criterias listed in the second column are extracted from several research papers. The malware names mentioned in the figure 1 are names that Symantec uses them for referring to them as the table is prepared based on information presented in Symantec website. The mentioned figure can be found in the next page.



		Backdoor. Rustock.B (2006)	W32. Virut (2007)	W32. Koobface (2008)	Backdoor. Tidserv (2008)	W32. Qakbot (2009)	W32. Pilleuz (2009)	Trojan. Zbot (2010)	Trojan. Carberp.B (2014)
System modification categories	File/Folder created	✓		✓	✓	✓	✓	✓	✓
	Files/Folder deleted				✓		✓		
	Files/Folder modified		✓		✓	✓	✓		
	Registry entries created	✓	✓	✓	✓	✓	✓	✓	✓
	Registry entries deleted								
	Registry entries modified								
	Kernel Modification	✓							
	Code Injection into process/DLL/Apps	✓	✓	✓	✓	✓	✓	✓	
Network category activities	Download additional files as updates or for local secondary infection	✓	✓	✓	✓	✓	✓	✓	
	Download advertisment or use user's info for advertisement purposes			✓	✓	✓			
	Upload stolen information to remote location		✓	✓	✓	✓	✓	✓	✓
	Block access to specific domains			✓	✓	✓		✓	
	Redirecting outbound internet trrafic to specific domains by modifying host file or re-routing the traffic	✓		✓	✓	✓			
	Spam activity	✓						✓	✓
	Mass downloads of a particular pay-per-install application and profit making intentions		✓	✓	✓				
	Network flood activities such as DDOS		✓				✓		

Figure 1: Comparison of botnet intended malware functionalities