ABSTRACT

MALWARE DETECTION ANALYSIS OF REMOTE ACCESS TROJAN WITH BEHAVIOUR-BASED DYNAMIC MALWARE ANALYSIS DETECTION TOOLS

By

EPIFANIO JUANG VICTORIUS

1202150100

The more the development of a technology, the greater the chance of cybercrime through malware attacks. Malicious software (malware) is a malicious software intentionally designed to run unfamiliar loads that harm or damage the victim's system without his knowledge. With many malware categories spread, making all systems vulnerable to malware attacks. One of the most dangerous categories of malware is Remote Access Trojan (RAT) which can control the system as a whole to steal personal information, delete files, modify files, disrupt user performance, and install malware or backdoor in the system. Evidenced by the existence of 557 RAT malware attacks that occur or are detected between September 1, 2017 to August 31, 2018 in several agencies or individuals in the United Kingdom. Therefore, malware analysis based behavior is needed to find out and analyze the unique malware behavior in the form of Windows API and Registry from malware RAT. This study uses 3 out of 10 RAT malware samples that have been obtained, namely DarkComet-RAT, njRAT, and QuassarRAT to be tested and analyzed for malware behavior. The malware behavior analyzed is the Windows API and Windows Registry when RAT malware is initiated, and executes Keylogger, File Transfer and The remote. Desktop uses dynamic malware analysis detection tools based on behavior. This study also compares the behavior of initiation between remote access software, namely AeroAdmin and malware RAT to find out the differences between the Windows API and the Windows Registry used. The malware behavior found explains that malware RAT will use the Windows API and Registry related to RPC and OLE to establish connections with targeted systems, then use the Windows API and Windows Registry related to Keyboard Input, Data Access and Storage, Graphic and Gaming when several features are executed. Malware RAT will not validate all activities carried out and all malware RAT features can be run manually by the attacker.

Keywords: *malware, malware rat, malware analysis, dynamic malware analysis, malware behaviour.*