# smokeloader_technical_analysis_report.pdf



## Sida 3 av 17

INTRODUCTION

The SmokeLoader family is a type of malware that belongs to the loader type. The main purpose of the program is to inject a more effective and destructive malware into the machine. First revealed in 2011, SmokeLoader is a family that is evolving day by day, using new techniques and constantly updating.

SmokeLoader is a family that aims to be keylogger, information theft, botnet, backdoor access on systems. In fact, it can be used for any harmful activity for the purpose of the attacker. It is spread through emails and drive-by download.

In the world of malware, PROPagate Injection has been used by SmokeLoaders for the first time. PROPagate injection, injects confidential code into an application other than the actual running application, allowing the malicious code to be run by a different application.

2