qakbot_technical_analysis_report.pdf

Sida 3 av 21

2

Introduction

Qakbot, which was first detected in 2007, is also known as QBOT. The main purpose of the QAKBOT family, is to steal credentials and other financial information about bank accounts. The QAKBOT family has become an effective cyberattack tool with data theft in recent years. This is how today's most dangerous cyber attacks can be carried out. Prolock can make banking transactions via IP address by remotely connecting to ransomware and Windows system. It can work and develop acting worm-like, create backdoors on machines, and record user input outputs.

Resurrected by other malware such as EMOTET, QAKBOT has been found to have been distributed through a spam campaign using spam or hidden emails. These cyberattacks primarily redirect to a malicious web page and use an Excel document as a dropper. Later, QAKBOT downloads the main malicious file with the help of macro codes in the excel document, which is the dropper. Droppers are a malicious component that works to download the actual ransomware. Droppers leaves a copy of itself on the machine and creates a scheduled task for autorun recording and persistence. It also injects itself into the explorer.exe process.

First Look

First, it starts with specialized phishing e-mail. The content of the mail is an Office document. The macros of office documents is written in VBScript. VBScript, modelled by Microsoft on Visual Basic, represents an Active Scripting language and downloaded contents enables communication with the server controlled by cybercriminals and command transmission.
