Breaking Dridex Malware

Published: 2021-06-03 · Archived: 2026-04-05 16:22:03 UTC

Speakers: Felipe Domingues, Security Researcher, AppGate | Brasil Gustavo Palazolo, Security Researcher, AppGate | Brasil Dridex is a major banking trojan that appeared somewhere around 2011, continually evolving ever since. In this presentation, we will cover Dridex's most recent and interesting functionalities, such as how it's deployed, anti-analysis tricks, and how to automate the IOCs extraction through reverse engineering. Finally, we will also show malware analysis can be used to find flaws in the malicious code, and how that can be used to create a vaccine to prevent the execution of the malware. About the Speakers Felipe Duarte Domingues and Gustavo Palazolo are security researchers at AppGates' Malware Analysis & Research Team (MART). AppGate is a Zero Trust industry leader named by The Forrester Wave, protecting many organizations around the world by providing secure access, digital fraud protection and defense\offense services. We spend most of our time analyzing digital threats to have a deep understanding of its functionalities and to create defensive measures to protect our customers. Gustavo Palazolo and Felipe Duarte Domingues are security researchers at AppGates' Malware Analysis & Research Team (MART). AppGate is a Zero Trust industry leader named by The Forrester Wave, protecting many organizations around the world by providing secure access, digital fraud protection and defense\offense services. We spend most of our time analyzing digital threats to have a deep understanding of its functionalities and to create defensive measures to protect our customers.
