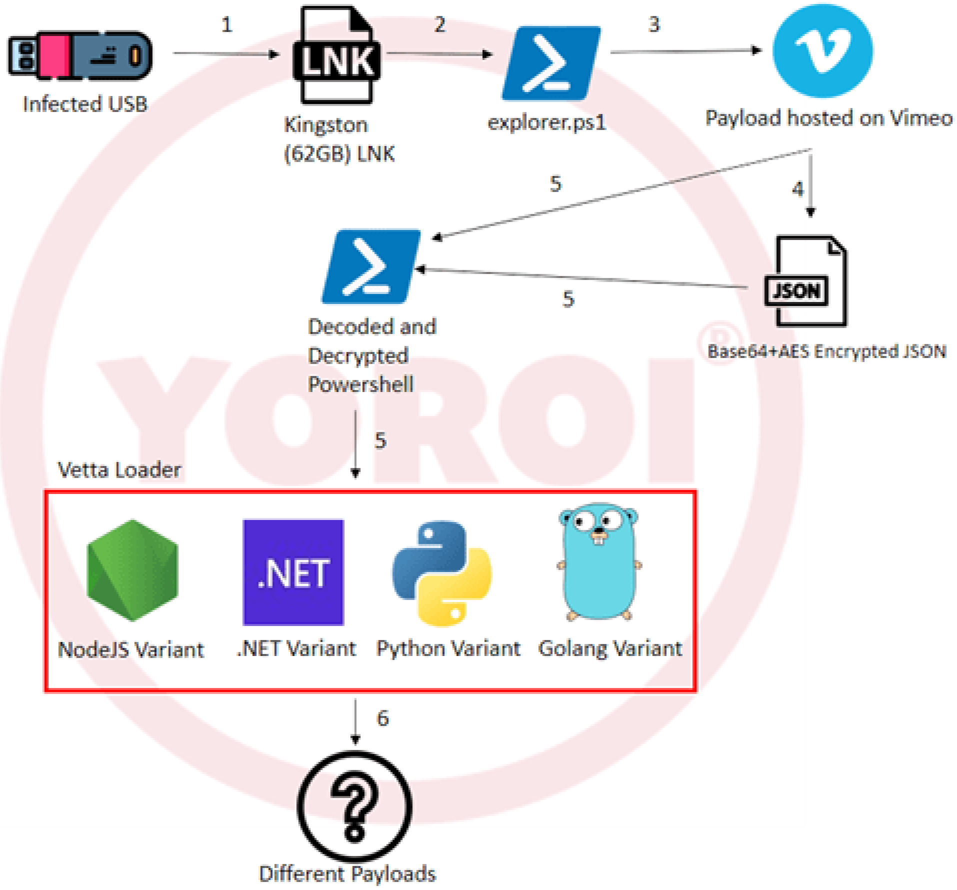
Unveiling “Vetta Loader”: A custom loader hitting Italy and spread through infected USB Drives

yoroi.company/en/research/unveiling-vetta-loader-a-custom-loader-hitting-italy-and-spread-through-infected-usb-drives/

December 6, 2023

In a recent investigation conducted by Yoroi's malware ZLab team, a persistent threat affecting several Italian companies, primarily in industrial, manufacturing, and digital printing sectors, has been unveiled. The modus operandi of this threat involves the utilization of infected USB drives, exploiting the heavy reliance on pen-drives for data sharing within these sectors.

The identified malware, named "Vetta Loader," employs public video services as a conduit for delivering its malicious payload. The report suggests a medium-high confidence level that the threat actor behind this campaign is Italian-speaking. Notably, the research uncovered four distinct variants of the Vetta Loader, each coded in different programming languages—NodeJS, Golang, Python, and .NET—while sharing a common approach to communication with command and control servers and subsequent stage downloads.



Vetta Loader infection chain

The infection chain analysis detailed in the report reveals the persistence and complexity of this threat. The prevalence of Vetta Loader on USB drives underlines their significance as a reliable means of malware distribution.

Yoroi recommends proactive measures to mitigate the risk associated with Vetta Loader. Users are advised to use only trusted USB drives, enable automatic antivirus scans, and consider the adoption of USB sanitizers. The report underscores the importance of understanding and addressing the unique challenges posed by malware distribution through USB drives, emphasizing the need for increased vigilance in sectors susceptible to such attacks.

Download Report

This Report has been authored by Luigi Martire, Carmelo Ragusa, Giovanni Pirozzi and Marco Giorgi