Severity

High

Analysis Summary

A Vietnam-based threat group, APT32 (OceanLotus Group) is active since 2014. It is known for carrying out sophisticated attacks on several private companies, journalists, foreign governments, and activists with a primary concentration on Southeast Asian countries including Vietnam, Philippines, Laos, and Cambodia. This threat group has utilized smart web breaches to compromise victims. APT32 conducts targeted operations that are consistent with Vietnamese state goals using a unique suite of fully-featured malware in combination with commercially accessible tools. The APT32 attack includes meaningless code to deceive security tools, allowing it to go undetected.

Impact

- Information Theft and Espionage
- Data Exfiltration

Indicators of Compromise

MD5

- 2cac346547f90788e731189573828c53

SHA-256

- 66b58b2afd274591fb8caf2dbfcf14d9c9bcf48d6c87e8df2db30cdefb0d1422

SHA-1

- df23328340d60fea800d4d21fa36837d7a7d5b72

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.