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

- 51d512e46de5ca5999f38d107349991b

SHA-256

- f892d7607e607f8dbad99d80d0d35ddd805c762bf3c02974e4fcf6a74949d069

SHA-1

- 3f71864de5a4bc21a6cb2811d325caf73a3e6a92

Remediation

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