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

- 38493746ae2f04110ee59dbbb5c17e1c

SHA-256

- 4c409e40d4830d41dc2c1e84a719a9da0c785ab86d751f35dba303aae2a7efa3

SHA-1

- 94783722c8585434a9a3ff34ecf91a0559d7161d

Remediation

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