Severity

High

Analysis Summary

The STOP/DJVU ransomware initially made headlines in 2018 and has since been attacking individuals all around the world. It's widespread on torrent sites and other platforms in software crack packages and adware bundles. The STOP/DJVU ransomware is a Trojan that encrypts files. It infiltrates your computer invisibly and encrypts all of your data, making them unavailable to you. It leaves a ransom letter warning which demands money in exchange for decrypting your data and making them available to you again. Malware is delivered via cracked applications, fake set-up apps keygens, activators, and Windows updates. It does not utilize local information like keyboard layouts or timezone settings to prevent infecting victims in certain countries; instead, it uses the information returned by a request to https[:]//api.2ip.ua/geo.json. The card's MAC address is utilized to provide unique identification for the system. This identity is provided to STOP's command and control server, which responded with an RSA-2048 public key for encryption. Additional malware, including an information stealer known as Vidar, is then downloaded and installed.

Impact

- Information Theft
- File Encryption

Indicators of Compromise

MD5

- 49cab554533fce29b45eb9f76f37577d
- d1f8b49a2f46e81a53759104e024c721

SHA-256

- d12dbc7ee849927f9ab857451c9ce420645993abce1d71bb61ea201013ad3a50
- b8f572649316a9695bd2691149019bcc79d33bb723176fb24bb464c8839bd5f4

SHA-1

- 8897b86bf6e694ac620d7d8b3b39b750b768dce7
- da36458f3ab7c94a365539603f0eadd5b23a9e1d

Remediation

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