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 that 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

- d600beac1e021639e589dd8cc6e428eb

SHA-256

- 051a2902c6a41210cbf84e97a4d24b7f4538414c25433e2e75ad0b6c9f7bf481

SHA-1

- d9e3e698d0a77905e6b577bbfdf1200a53f93af1

Remediation

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