DoNex Ransomware

Date: 19th March 2024 | Severity: High

Summary

The DoNex ransomware group, first reported by cybersecurity researchers in March 2024, has been active since at least February 2024. The ransomware group targets businesses within the United States and Europe.

After DoNex targets their victim, they utilize the double extortion method by not only encrypting victim files, but also adding them to their ransomware website with a distinct VictimID extension.

Once the victim is compromised, the DoNex ransomware group provides a ransom note, including means to communicate through Tox, a secure and anonymous communication method.

Attack Vectors

- The Several companies have been listed as victims of the DoNex ransomware organization on their dark web domain, which can be accessed through the Onion network, thereby establishing their presence. The gang uses a double-extortion technique, which makes its techniques sneakier.
- The encryption used by DoNex contains capable and stable features, such as restarting the machine, cleaning event logs, local and network file discovery, and shutting down processes that may interfere with the encryption of the target files.
- Most features in this encryptor utilize common Windows API and system commands to achieve their goal.

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	0adde4246aaa9fb3964d1d6cf3c29b1b13074015b250eb8e5591339f92e1e3ca[.] 2b15e09b98bc2835a4430c4560d3f5b25011141c9efa4331f66e9a707e2a23c0[.]
URL	http://g3h3klsev3eiofxhykmtenmdpi67wzmaixredk5pjuttbx7okcfkftqd.onion
Email	donexsupport@onionmail.org [.]

Recommendation

Submit the File Hash to the Antivirus team to update their database with the file hashes.

Submit the URL to the Network team to update their database with the URL.

Submit the Email to the Email security team to update their database with the Domains.

Make regular backups of important and critical files.

Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.

Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

https://dashboard.ti.insight.rapid7.com/#/tip/cyber-term/65f2038c44e8d12fafc353ea

https://www.ttbinternetsecurity.com/news/new-donex-ransomware-observed-in-the-world-targeting-enterprises?&web_view=true