DoNex Ransomware

Date: 13th May 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.

Attack Vectors

DoNex utilizes the double extortion method by not only encrypting victim files, but also adding them to its ransomware website with a distinct VictimID extension. Once the victim is compromised, DoNex deploys a ransom note, which includes means to communicate through Tox, a secure and anonymous communication method.

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 the threat actors' goal.

Indicator of compromise

INDICATOR TYPE	INDICATORS
URL	http[:]//g3h3klsev3eiofxhykmtenmdpi67wzmaixredk5pjuttbx7okcfkftqd.onion
Email	donexsupport@onionmail.orgt
File Hashes	• 6d6134adfdf16c8ed9513aba40845b15bd314e085ef1d6bd20040afd42e36e40 • 2b15e09b98bc2835a4430c4560d3f5b25011141c9efa4331f66e9a707e2a23c0 • b32ae94b32bcc5724d706421f915b7f7730c4fb20b04f5ab0ca830dc88dcce4e • fcad682ce067a2cdc077b4c39a05331d187482a2 • c55c60a23f5110e0b45fc02a09c4a64d3094809a • 900944b4eb076ee4bf9886bec81dce499b48d69b • cfc7b4d9933483c25141ba49b4d5755e • 318a50cb34cba9325dfd82d7e66394f2 • 8a10e0dc4994268ea33baecd5e89d1e2ddabef30afa09961257a4329669e857a • 4b4052b50144f00a9168a4ad02de29e1bfb40b6e

INDICATOR TYPE	INDICATORS
File Hashes	• 74b5e2d90daaf96657e4d3d800bb20bf189bb2cf487479ea0facaf6182e0d1d3 • cb1c423268b1373bde8a03f36f66b495 • 0e60d49a967599fab179f8c885d91db25016be996d66a4e00cbb197e5085efa4 • 8939bfe20bc6476806d22c8edfcaba5c36f936b893b3de1c847558502654c82f • 21eae7e488b145fa3618627da99c3234696c0f15 • 892cd69f889b25cb8dc11b0ac75c330b6329e937 • 191b3b39f3893ea272a45dd42cda297831db58a6 • 1933fed76a030529b141d032c0620117 • 1940fcdb2561c2f7b82f6c44d22a9906e5ffec2438d5dadfe88d1608f5f03c33 • 0adde4246aaa9fb3964d1d6cf3c29b1b13074015b250eb8e5591339f92e1e3ca • 45ec0c61105121da6fed131ba19a463b • 9dfdd81f5948ea52879a12ba039881bb • 8a23347b733420472a1ec0a1eeada597 • d3997576cb911671279f9723b1c9505a572e1c931d39fe6e579b47ed58582731

Recommendation

- Educating employees about the dangers of sponsored ads and the importance of verifying software through official channels.
- Deploy Endpoint Detection and Response (EDR) solutions across all devices.
- Implement Phishing and Security Awareness Training (PSAT) program.
- Control MSIX execution via AppLocker policies.
- Report incidents of certificate misuse by threat actors.

Reference Links

- https://dailysecurityreview.com/security-spotlight/new-donex-ransomware-targets-enterprises/
- https://www.ttbinternetsecurity.com/news/new-donex-ransomware-observed-in-the-world-targeting-enterprises?&web_view=true
- https://www.pcrisk.com/removal-guides/29294-donex-ransomware