Severity

Medium

Analysis Summary

Introduction:

A state-sponsored North Korean threat actor group with techniques similar to the previously disclosed Lazarus Group (AppleJeus) is identified by governments. Through the distribution of cryptocurrency trading applications, Lazarus leveraged AppleJeus to trojanize cryptocurrency applications, primarily targeting cryptocurrency exchanges and financial services firms. The Lazarus Group has targeted a number of blockchain and cryptocurrency firms, entities, and exchanges. To fund their regime, these actors will continue to exploit the vulnerabilities of cryptocurrency technology firms, gaming companies, and exchanges.

North Korean cyber actors are observed targeting blockchain technology and cryptocurrency companies, including cryptocurrency exchanges, decentralized finance (DeFi) protocols, cryptocurrency trading companies, venture capital funds investing in cryptocurrency, and valuable non-fungible tokens (NFTs). This State-Sponsored APT group utilizes spear-phishing mails delivered over numerous communication platforms to employees of cryptocurrency companies. The mails frequently resemble a recruiting drive and offer high-paying employment in order to persuade recipients to download malware-laced cryptocurrency programs known as “TraderTraitor” by the U.S. government. The term TraderTraitor refers to a set of malicious applications written using cross-platform JavaScript code with the Node.js runtime environment. Websites with modern designs are used in these campaigns to promote the alleged features of the software. — CISA

Impact

- Cryptocurrency Theft
- Financial Theft

Indicators of Compromise

Domain Name

- dafom[.]dev
- tokenais[.]com
- cryptais[.]com
- alticgo[.]com
- esilet[.]com
- greenvideo[.]nl
- dafnefonseca[.]com
- haciendadeclarevot[.]com
- sche-eg[.]org
- www[.]vinoymas[.]ch
- infodigitalnew[.]com
- creaideck[.]com
- aideck[.]net

IP

- 45[.]14[.]227[.]58
- 199[.]188[.]103[.]115
- 82[.]102[.]31[.]14
- 108[.]170[.]55[.]202
- 104[.]168[.]98[.]156
- 151[.]101[.]64[.]119
- 185[.]66[.]41[.]17

- 160[.]153[.]235[.]20
- 38[.]132[.]124[.]161
- 89[.]45[.]4[.]151

MD5

- c2ea5011a91cd59d0396eb4fa8da7d21
- 930f6f729e5c4d5fb52189338e549e5e
- 4e5ebbecd22c939f0edf1d16d68e8490
- 1c7d0ae1c4d2c0b70f75eab856327956
- 855b2f4c910602f895ee3c94118e979a
- 9a6307362e3331459d350a201ad66cd9
- 53d9af8829a9c7f6f177178885901c01
- 1ca31319721740ecb79f4b9ee74cd9b0
- 9578c2be6437dcc8517e78a5de1fa975
- 5d43baf1c9e9e3a939e5defd8f8fbd8d
- 8397ea747d2ab50da4f876a36d673272

SHA-256

- 60b3cfe2ec3100caf4afde734cfd5147f78acf58ab17d4480196831db4aa5f18
- 5b40b73934c1583144f41d8463e227529fa7157e26e6012babd062e3fd7e0b03
- f0e8c29e3349d030a97f4a8673387c2e21858cccd1fb9ebbf9009b27743b2e5b
- 765a79d22330098884e0f7ce692d61c40dfcf288826342f33d976d8314cfd819
- e3d98cc4539068ce335f1240deb1d72a0b57b9ca5803254616ea4999b66703ad
- 8acd7c2708eb1119ba64699fd702ebd96c0d59a66cba5059f4e089f4b0914925
- 9ba02f8a985ec1a99ab7b78fa678f26c0273d91ae7cbe45b814e6775ec477598
- 9d9dda39af17a37d92b429b68f4a8fc0a76e93ff1bd03f06258c51b73eb40efa
- dced1acbbe11db2b9e7ae44a617f3c12d6613a8188f6a1ece0451e4cd4205156
- 867c8b49d29ae1f6e4a7cd31b6fe7e278753a1ba03d4be338ed11fd1efc7dd36
- 89b5e248c222ebf2cb3b525d3650259e01cf7d8fff5e4aa15ccd7512b1e63957

SHA-1

- b2d9ca7b6d1bbbe4864ea11dfca343b7e15597d8
- 8e67006585e49f51db96604487138e688df732d3
- f1606d4d374d7e2ba756bdd4df9b780748f6dc98
- f3263451f8988a9b02268f0fb6893f7c41b906d9
- ff17bd5abe9f4939918f27afbe0072c18df6db37
- 3f2c1e60b5fac4cf1013e3e1fc688be490d71a84
- ae9f4e39c576555faadee136c6c3b2d358ad90b9
- 41f855b54bf3db621b340b7c59722fb493ba39a5
- d2a77c31c3e169bec655068e96cf4e7fc52e77b8
- d5ff73c043f3bb75dd749636307500b60a436550
- 48a6d5141e25b6c63ad8da20b954b56afe589031

Remediation

- Emails from unknown senders should always be treated with caution.
- Never open links or attachments from unknown senders
- Block all threat indicators at your respective controls.
- Look for IOCs in your surroundings.