Hive Pro

THREAT ADVISORY

Lazarus is back, targeting organizations with cryptocurrency thefts via TraderTraitor malware

TA2022097

Threat Level RED

Publish Date – April 19, 2022

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Treasury Department (Treasury) have issued a joint Cybersecurity Advisory(CSA) to make organizations in the blockchain technology and cryptocurrency industry aware of a cyber threat associated with cryptocurrency attacks and phishing campaign carried out by Lazarus Group, a North Korean state-sponsored advanced persistent threat (APT) group.

The initial attack begins with sending a thousands of phishing emails to individuals of the targeted firm. They are tempted by good job opportunities - a common tactic used by the Lazarus APT to convince individuals to download trojanized cryptocurrency applications on Windows or macOS operating systems. The trojanized applications include TokenAIS, CryptAIS, and Esilet is loaded with TraderTraitor malware. These apps are cross-platform, Electron-based platform utilities created with the Node.js and JavaScript runtime environments. When the payload is executed, the attacker gains access to the victim's computer and company network by executing commands and sending additional malware.

The MITRE ATT&CK TTPs used by **Lazarus** are:
TA0001: Initial Access
TA0005: Defense Evasion
TA0002: Execution
TA0040: Impact
TA0004: Privilege Escalation
TA0006: Credential Access
TA0009: Collection
TA0003: Persistence
T1204: User Execution
T1553: Subvert Trust Controls
T1566: Phishing
T1566.002 Spear phishing Link
T1059: Command and Scripting Interpreter
T1059.007: Command and Scripting Interpreter: JavaScript
T1496: Resource Hijacking
T1134: Access Token Manipulation
T1110: Brute Force
T1140: Deobfuscate/Decode Files or Information
T1113: Screen Capture
T1543: Create or Modify System Process
T1486: Data Encrypted for Impact

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
Lazarus Group APT38, BlueNoroff, and Stardust Chollima	North Korea	Worldwide	Blockchain technology and cryptocurrency industry, Financial, Critical Infrastructure, Government, Gaming, Financial Services, Technology	Financial Crime

Indicators of Compromise (IoCs)

Type	Value
Domain	tokenais[.]com, esilet[.]com, dafom[.]dev, cryptais[.]com, creaideck[.]com, alticgo[.]com, aideck[.]net, greenvideo[.]nl, dafnefonseca[.]com, haciendadeclarevot[.]com, sche-eg[.]org, vinoymas[.]ch, infodigitalnew[.]com, creaideck[.]com, darwin64.bin
File name	DAFOM-1.0.0[.]dmg TokenAIS.app[.]zip, CryptAIS[.]dmg, AlticGO[.]exe, AlticGO_R.]exe, Esilet.dmg, Esilet-tmpzpsb3, silet-tmpg7lpp, win32.bin
IPV4	108.170.55[.]202, 199.188.103[.]115, 82.102.31[.]14, 108.170.55[.]202, 104.168.98[.]156, 62.84.240[.]140, 151.101.64[.]119, 185.66.41[.]17, 160.153.235[.]20, 46.16.62[.]238, 107.154.160[.]132, 38.132.124[.]161
Hostname	www[.]esilet[.]com, www[.]alticgo[.]com, www.vinoymas[.]ch
URLs	https: //infodigitalnew.com/wp-content/plugins/top[.]php, https: //greenvideo.nl/wp-content/themes/top[.]php, https: //dafnefonseca.com/wp-content/themes/top[.]php, https: //haciendadeclarevot.com/wp-content/top[.]php, https: //sche-eg.org/plugins/top[.]php, https: //www[.]vinoymas.ch/wp-content/plugins/top[.]php

Type	Value
MD5	c2ea5011a91cd59d0396eb4fa8da7d21, 9a6307362e3331459d350a201ad66cd9, 9578c2be6437dcc8517e78a5de1fa975, 930f6f729e5c4d5fb52189338e549e5e, 855b2f4c910602f895ee3c94118e979a, 8397ea747d2ab50da4f876a36d673272, 5d43baf1c9e9e3a939e5defd8f8fbd8d, 53d9af8829a9c7f6f177178885901c01, 4e5ebbecd22c939f0edf1d16d68e8490, 1ca31319721740ecb79f4b9ee74cd9b0, 1c7d0ae1c4d2c0b70f75eab856327956
SHA1	ff17bd5abe9f4939918f27afbe0072c18df6db37, f3263451f8988a9b02268f0fb6893f7c41b906d9, f1606d4d374d7e2ba756bdd4df9b780748f6dc98, d5ff73c043f3bb75dd749636307500b60a436550, d2a77c31c3e169bec655068e96cf4e7fc52e77b8, b2d9ca7b6d1bbbe4864ea11dfca343b7e15597d8, ae9f4e39c576555faadee136c6c3b2d358ad90b9, 8e67006585e49f51db96604487138e688df732d3, 48a6d5141e25b6c63ad8da20b954b56afe589031, 41f855b54bf3db621b340b7c59722fb493ba39a5, 3f2c1e60b5fac4cf1013e3e1fc688be490d71a84
SHA256	f0e8c29e3349d030a97f4a8673387c2e21858cccd1fb9ebbf9009b27743b2e5b, e3d98cc4539068ce335f1240deb1d72a0b57b9ca5803254616ea4999b66703ad, dced1acbbe11db2b9e7ae44a617f3c12d6613a8188f6a1ece0451e4cd4205156, 9d9dda39af17a37d92b429b68f4a8fc0a76e93ff1bd03f06258c51b73eb40efa, 9ba02f8a985ec1a99ab7b78fa678f26c0273d91ae7cbe45b814e6775ec47759,8 8acd7c2708eb1119ba64699fd702ebd96c0d59a66cba5059f4e089f4b0914925, 89b5e248c222ebf2cb3b525d3650259e01cf7d8fff5e4aa15ccd7512b1e63957, 867c8b49d29ae1f6e4a7cd31b6fe7e278753a1ba03d4be338ed11fd1efc7dd36, 765a79d22330098884e0f7ce692d61c40dfcf288826342f33d976d8314cfd819, 60b3cfe2ec3100caf4afde734cfd5147f78acf58ab17d4480196831db4aa5f18, 5b40b73934c1583144f41d8463e227529fa7157e26e6012babd062e3fd7e0b03

References

https://www.cisa.gov/uscert/ncas/alerts/aa22-108a