Ransomware Security Bulletin

DIR Cybersecurity Incident Response Team (CIRT)
Feb 9, 2023

SUBJECT: Ransomware Attacks on Critical Infrastructure Fund DPRK Espionage Activities

TLP: CLEAR

Announcement ID: 1189777
Date: 2/09/2023
Announcement Type: Cybersecurity Advisory
Importance: Standard
Distributed to: TX-ISAO: Everyone

OVERVIEW:

CISA, the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Department of Health and Human Services (HHS), and Republic of Korea's Defense Security Agency and National Intelligence Service have released a joint Cybersecurity Advisory (CSA), Ransomware Attacks on Critical Infrastructure Fund DPRK Espionage Activities, to provide information on ransomware activity used by North Korean state-sponsored cyber to target various critical infrastructure sectors, especially Healthcare and Public Health (HPH) Sector organizations.

The authoring agencies urge network defenders to examine their current cybersecurity posture and apply the recommended mitigations in this joint CSA, which include:

- Train users to recognize and report phishing attempts.
- Enable and enforce phishing-resistant multifactor authentication.
- Install and regularly update antivirus and antimalware software on all hosts.

See Ransomware Attacks on Critical Infrastructure Fund DPRK Espionage Activities for ransomware actor's tactics, techniques, and procedures, indicators of compromise, and recommended mitigations. Additionally, review StopRansomware.gov for more guidance on ransomware protection, detection, and response.

TLP:CLEAR = Recipients can spread this to the *world*, there is no limit on disclosure.

TLP: CLEAR

Sources may use TLP:**CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:**CLEAR** information may be shared without restriction.

https://www.us-cert.gov/tlp

Assistance/Feedback/Questions?

Texas Information Sharing and Analysis Organization

DIRSecurity@dir.texas.gov

Submit a Threat Report

Texas ISAO Threat Reporting System

Sign up for News and Intelligence

TX-ISAO Mailing List Access Request Form

Texas Department of Information Resources

www.dir.texas.gov

Transforming How Texas Government Serves Texans