Critical Infrastructure Partners,

In partnership with the FBI, Treasury, and FinCEN, CISA published a joint Cybersecurity Advisory (CSA) with recommended actions and mitigations for organizations to take to protect against reported tactics, techniques, and procedures (TTPs) by Karakurt data extortion group that has been creating significant challenges for defense and mitigation.

Karakurt victims have not reported encryption of compromised machines or files; rather, Karakurt actors claimed to steal data and threatened to auction it off or release it to the public unless they receive payment of the demanded ransom. As of May 2022, several terabytes worth of data purported to belong to victims across North America and Europe, along with several "press releases" naming victims who had not paid or cooperated, and instructions for participating in victim data "auctions" was reported to be contained on Karakurt operated website located in the deep web and on the dark web.

During reconnaissance, Karakurt actors appear to obtain access to victim devices, primarily, by purchasing stolen login credentials. They can also obtain access to already compromised victims from cooperating partners in the cybercrime community or buying access to already compromised victims via third-party intrusion broker networks.

Actions that organizational leaders and network administrators can take today to mitigate cyber threats from ransomware include prioritizing patching known exploited vulnerabilities, training users to recognize and report phishing attempts, and enforcing multi-factor authentication (MFA). More recommended mitigations include:

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location.
- Implement network segmentation and maintain offline backups of data to ensure limited interruption to the organization.
- Regularly back up data and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Install and regularly update antivirus software on all hosts and enable real time detection.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized accounts.

Organizations are encouraged to review the advisory for all the details on the Karakurt actors, associated indicators of compromise, malicious behavior mapped to MITRE ATT&CK, and agency resources available to all organizations.

All organizations should share information about incidents and unusual cyber activity with CISA and/or FBI. When cyber incidents are reported quickly, it can contribute to stopping further attacks. Organizations should inform CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870, or an FBI field office.

Your support to amplify this advisory through your communications and social media channels is appreciated. And as always, thank you for your continued collaboration.

v/r,

Janine Mason (she/her)
Section Chief (A), Chemical, Stakeholder Engagement Division
Cybersecurity and Infrastructure Security Agency
M: 202.213.0405 | janine.mason@cisa.dhs.gov |chemicalsector@cisa.dhs.gov