Cain & Associates

Nov 13th, 2022

To Whom it may concern:

In early October of 2022, Cain & Associates was tasked to assist Los Angeles District Attorney's Office Bureau of Investigation in the execution of a court-ordered search warrant against Konnech, Inc and its CEO Eugene YU. We were hired to provide specialized capabilities which are defined as Highly Adaptable Cybersecurity Services (HACS). These services included the use of Cyber-Forensics, Live Capture, Search Find & Recovery, Data Examination/Analysis, Network Enumeration & Security, and Advanced Persistent Threat (APT) analysis of Foreign Adversaries. We feel it necessary to report the following to Federal, State, and local law enforcement authorities, election, and other necessary government officials, regarding same, those that may be affected by the findings of our investigation.

Following the search and seizure of computer based assets in Michigan, and at the instruction of the Investigating Officer (IO), we logged into accounts with credentials that were provided to us and continued a live capture operation over a number of days utilizing forensic methods currently in use by federal law enforcement agencies, maintaining complete and accurate chain of evidence and a complete live screen capture of all of our work in order to preserve its admissibility in court. In addition to screen captures, we were able to recover a trove of files from the provided accounts. While the files we had access to were not the entire databases involved, it was significant in that it confirmed multiple instances of US persons' (USPs) personally identifiable information (PII) being hosted on Chinese servers. Cain and Associates also found significant evidence in private company messages that software code was being developed, tested and maintained in China. We also observed administrative credentials being passed to Chinese developers. Under Justice Department guidelines this would constitute a Type 2 data breach where the company lost total control of the data and systems. During the investigation Cain and Associates found evidence of a potential foreign adversary intelligence operation inside Konnech infrastructure connected to Chinese IP addresses. This warranted Cain & Associates to file a national security emergency information of "URGENT CONCERN" to the Defense Counterintelligence Security Agency (DCSA) IAW SEAD 3 requirements for contractors with active US Security Clearances. Below is a summary of our observations:

1. Cain & Associates observed evidence that US persons and non-US persons located in People's Republic of China (PRC), associated with Konnech, had shared information, including but not limited to, PII of election workers, PII of registered voters, PII of election judges, and sensitive election equipment inventory information (hereby referred to as "Election Related Data") of at least 6 or more separate US counties.

2. Cain & Associates observed Konnech employing non-US persons to perform coding/programming/software development work on election worker management systems, located both inside and outside the United States.
    - Many of these employees appeared to be Chinese nationals based on social media, profiles, listed phone numbers, and listed locations in the data we observed.
    - All Konnech employees and Chinese developers were at one time given privileged access to these systems, this almost certainly gave them access to US persons PII due to a misconfiguration allowing them to change their own role to "Superuser".

3. Cain & Associates observed that Konnech automatically imported, as well as linked their websites to Scytl, a Spanish Government funded company, which has been involved in many controversies to include election voting fraud.

4. Cain & Associates observed that Konnech employees have shared election related data through, from, and on Chinese servers/applications which are stored for up to 180 days.

5. Cain & Associates observed evidence in metadata pulled from files that indicated Eugene YU was involved in the development of the Chinese government (i.e.,Wucheng District People's Congress) election software.

6. Cain and Associates observed organizational structure that Konnech is connected with a number of companies residing in mainland China. These companies appear to be linked to and subsidized by the PRC government as indicated by PRC government documents recovered and reviewed by our team:
    - Wuhan Yiqing Technology Co., Ltd.
    - Jinhua R&D Center
    - Wuhan R&D Center

It must be emphasized that there have been no hearings or interviews with the suspects regarding this evidence to our knowledge although this might have happened without our knowledge. Further, the company and Eugene YU are still afforded the full rights of any defendant in the United States to defend themselves against any such suspicions. That said, Konnech employees and contractors appear to be violating numerous laws and regulations regarding US critical infrastructure. These would include Information and Communications Technology and Services (ICTS) Supply Chain transactions between US and foreign persons that pose an undue or unacceptable risk and "involve information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary."

Cain and Associates is ready and willing to cooperate with any legal investigations where an official investigation is underway, and the agency agrees to keep the data confidential. If you or your organization are interested in engaging with Cain & Associates on this or any other cyber related investigative matters, please contact us via email at investigations@cain.associates or via mail at PO Box 783, Hedgesville, WV, 25427-0783