SIXGILL REPORT

Hacked Chinese Rail Control System

March 3, 2019

Hacked Chinese Rail Control System

As part of our day-to-day work on Sixgill's threat intelligence platform, Sixgill's Intelligence team identified a potential threat to a rail control system in China.

On February 19th, 2019, an actor operating on a top-tier dark web forum shared an offer to sell access to the admin panel of a Chinese rail control system. The hacked entity manufactures, among other things, safety management systems for rail transportation, as well as management systems for the aviation sector.

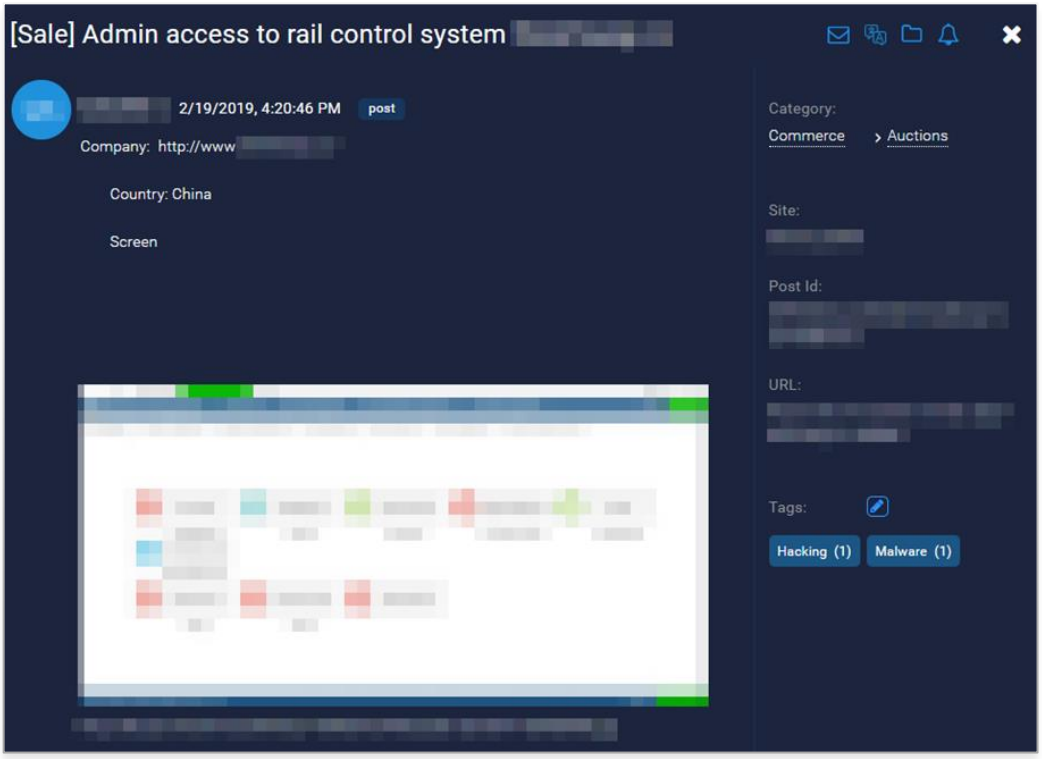

Figure 1: Post of admin access for sale to a rail control system in China, as seen on the Sixgill platform.

The threat actor shared the post in English on a Russian-speaking forum, and provided visual proof of the offered admin access, sharing four print-screens of the hacked management system. The screenshots include the system configuration, information management and personnel management, which allow further access to the module, navigation, and employee management systems, as well as the codes for locomotive segments.

This post exemplifies the growing trend of hacked ICS systems. With the kind of information provided in the post, the attacker is able to access the management software and damage its activity, potentially resulting in the loss of life. Furthermore, hacking into a specific rail control system suggests

that the actor has the know-how needed to hack into other organizations that use the same or similar management systems.

As the use of such control systems becomes more prevalent, the cyber threats against them grow. From threat actors who explore new ways of making a profit, to terrorists who seek to execute attacks that will inflict massive damage, attacks on ICS have become a major threat to many organizations and governments.