New ‘LazyScripter’ Hacking Group Targets Airlines

By Ionut Arghire

Published: 2021-02-24 · Archived: 2026-04-05 21:14:49 UTC

A recently identified threat actor that remained unnoticed for roughly two years appears focused on the targeting of airlines that are using the BSPLink financial settlement software made by the International Air Transport Association (IATA), cybersecurity firm Malwarebytes reported on Wednesday.

Initially identified in December 2020, the threat actor is targeting IATA and airlines, with the most recent attacks employing a phishing lure mimicking the newly introduced IATA ONE ID (Contactless Passenger Processing tool).

Dated 2018, one of the earliest attacks attributed to the adversary, which Malwarebytes refers to as LazyScripter, was aimed at individuals looking to immigrate to Canada. Over time, the group evolved its toolset from PowerShell Empire to the Koadic and Octopus RATs, and used LuminosityLink, RMS, Quasar, njRat and Remcos RATs in between.

The phishing emails used in these attacks used the same loader to drop both Koadic and Octopus. Referred to as KOCTOPUS, it was preceded by Empoder, a loader for PowerShell Empire.

IATA- or job-related themes were typically used as lures, but additional lures were also observed: IATA security, IATA ONE ID, user support kits for IATA users, BSPlink Updater or Upgrade, Tourism (UNWTO), COVID-19, Canada skill worker program, Canada Visa, and Microsoft Updates.

The phishing emails carry either archive or document files containing a variant of a loader. The malicious tools were mainly hosted using two GitHub accounts, both deleted on January 12 and 14, 2021, respectively, with a new account being created on February 2.

The latest campaign launched by the threat actor was spotted on February 5, with a variant of KOCTOPUS being delivered, masquerading as BSPLink Upgrade.exe. In addition to Octopus and Koadic, the loader also delivered a variant of Quasar RAT.

Malwarebytes' researchers have identified 14 malicious documents that the threat actor has used since 2018, all carrying embedded objects that are variants of the KOCTOPUS or Empoder loaders.

To date, the researchers have identified four different versions of the KOCTOPUS loader, used to load Octopus, Koadic, LuminosityLink, RMS, and Quadar RATs.

The Koadic RAT is known to have been previously used by the Iran-linked Muddy Water and Russia-linked APT28 threat actors. Malwarebytes was able to identify some similarities between the activities of LazyScripter and Muddy Water, but also a series of differences that resulted in the tracking of this group separately.

Related: Elusive Lebanese Threat Actor Compromised Hundreds of Servers

Related: Chinese Threat Actor 'Mustang Panda' Updates Tools in Attacks on Vatican

Related: U.S. Shares Information on North Korean Threat Actor 'Kimsuky'

Source: https://www.securityweek.com/new-lazyscripter-hacking-group-targets-airlines/