40,000 CryptBot Downloads per Day

By Karsten Hahn

Published: 2020-02-27 · Archived: 2026-04-05 15:45:51 UTC

AutoHotkey Downloader

We found the Bitbucket repository via a malicious AutoHotkey downloader[1]. The AutoHotkey script is located in the PE resources with the RCDATA resource type. We used Resource Hacker to access the script (see image below).

The downloader checks IP and location information of the infected system via http://ip-api.com/line/ and puts the result into %TEMP%/ip_.txt. Then it calls two shortened URLs at https://iplogger.org. This URL shortener service provides statistics and location tracking for the shortened links. The site's content is downloaded to %TEMP%/loger.txt and %TEMP%/loger2.txt.

It proceeds to check the country code in ip_.txt and will download PCBoosterSetup.exe[8] for the following country codes: TR, FR, US, DE, GB, HR, HU, RO, PL, IT, PT, ES, CA, DK, AT, NL, AU, AR, NP, SE, BE, NZ, SK, SO, GR, BG
