Intel Report #20190929_025248

Date:

2019-09-29 02:52:48

Description:

On 2019-09-29, a password cracking attack via SSH was attempted against a company named GROVE HILL located in the country of Clhos. The attacker used the tool, Hydra, during its attack. Although only a single user account was compromised in the attack, it is believed the attack was an unsuccessful attempt to display military prowess. One of the indicators discovered was the IPv4 address, 180.234.206.83. The attacker also attempted to install the malware CoinTicker on the compromised computer system.

Possible attribution

Overimaginative Xerxes