Severity

High

Analysis Summary

Evilnum is a financial-motivated APT group that has been active since 2018. This group has been involved in several attacks throughout its brief history while its targets stayed constant. Evilnum has been pursuing financial technology startups and will continue to do so. They have mostly targeted companies in the EU and the United Kingdom, while there have been instances of targets in Canada and Australia. One of the new additions to Evilnum's arsenal is PyVil RAT, a remote access trojan built-in Python, according to the researchers.

Impact

- Exposure of Sensitive Data
- Information Theft and Espionage

Indicators of Compromise

MD5

- eaec514c30e7139b1540c6ce5a7e36ad

SHA-256

- 43eda4ff53eef4513716a5b773e6798653ee29544b44a9ae16aa7af160a996f2

SHA-1

- d837d8e7d578c6efeed29f00f04966cc273a6603

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.