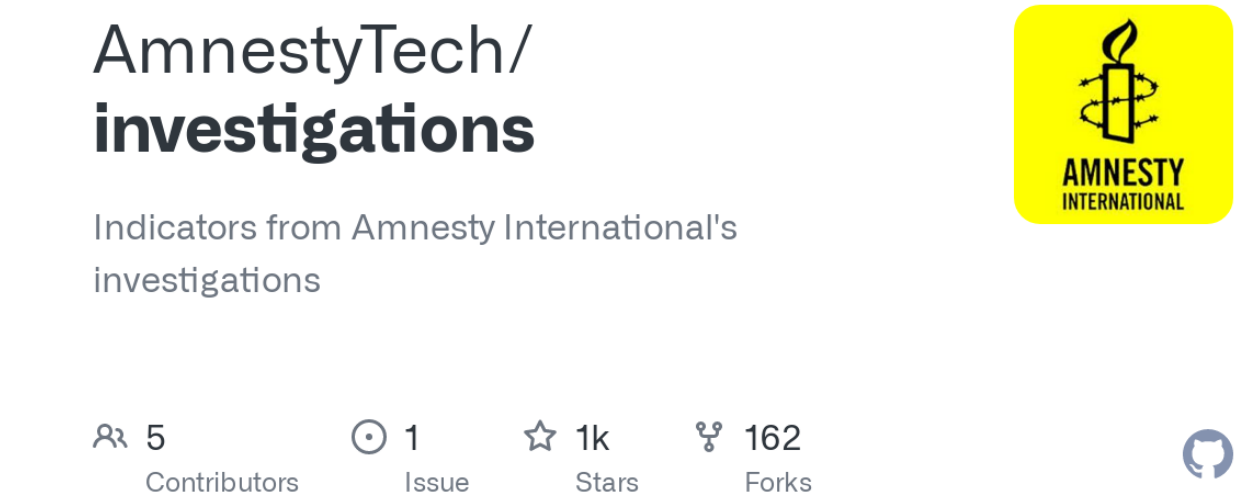
NSO Group Pegasus Indicator of Compromise

github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso

AmnestyTech



This repository contains network and device indicators of compromised related to NSO Group's Pegasus spyware. These indicators are a result of multiple investigations by the Amnesty International Security Lab and other partners. Additional technical information was collected as part of a collaborative investigation, the Pegasus Project coordinated by Forbidden Stories and involving a global network of investigative journalists.

Amnesty International has released a Technical Methodology report which outlines how to use these indicators to hunt for Pegasus and other mobile spyware products. The Amnesty International Security Lab is also releasing an open-source tool, the Mobile Verification Toolkit (MVT). MVT can be used with the the pegasus.stix2 indicators to check a devices for potential signs of compromise with Pegasus spyware.

These indicators include:

- `domains.txt` : list of all Pegasus-related domains, with sub-files:
- `v2_domains.txt` : list of Pegasus Version 2 infrastructure. These domains were identifed and published previously by Citizen Lab
- `v3_domains.txt` : list of Pegasus Version 3 infrastructure
- `v4_domains.txt` : list of Pegasus Version 4 infrastructure
- `v4_validation_domains.txt` : list of Pegasus Version 4 validation/URL shortener domains

- `emails.txt` : list of iCloud accounts used for exploiting zero-click vulnerabilities in iMessage and other Apple apps
- `files.txt` : list of suspicious files
- `pegasus.stix2` : STIX v2 file containing IOCs that can be used with MVT
- `processes.txt` : list of Pegasus-related process names identified on compromised phones