Interactive Mapping of APT-C-23 - Check Point Research

By Dexter Eugenio

Published: 2018-08-27 · Archived: 2026-04-05 20:32:48 UTC

Research by: Aseel Kayal

Last month, we investigated the renewal of a targeted attack against the Palestinian Authority, attributed to the APT-C-23 threat group. Although this campaign was initially discovered in early 2017, it is still active today and has been using both desktop and mobile attack vectors throughout the past year.

Dubbed by Check Point Research as the 'Big Bang APT', due to its use of character names from the famous Big Bang Theory sitcom, the latest resurgence we discovered was certainly not the only one keen on using TV references. In fact, since its early days this has been a peculiar aspect of the constantly changing campaign with certain elements of the campaign often referring to actors and characters from well-known TV shows.

In order to monitor the evolution of this campaign and the similarities between its components, we have created a visualization of the C&C domains from all the generations of this attack, the reports they came from, and the connections between them.
Click here for the interactive Map.

This map keeps track of insights provided by different security vendors, and has been updated to include newer indicators of compromise that were found after we published our own research. So far, we were able to collect approximately 100 unique domains that were used by malware samples at different points in time.

It seems that whoever is behind this is not only making sure that they are releasing more advanced malware with stronger capabilities, but are also making drastic changes to the campaign's infrastructure in an attempt to evade detection by security vendors.

Go to the interactive map>>

Source: https://web.archive.org/web/20230604112435/https://research.checkpoint.com/2018/interactive-mapping-of-apt-c-23/