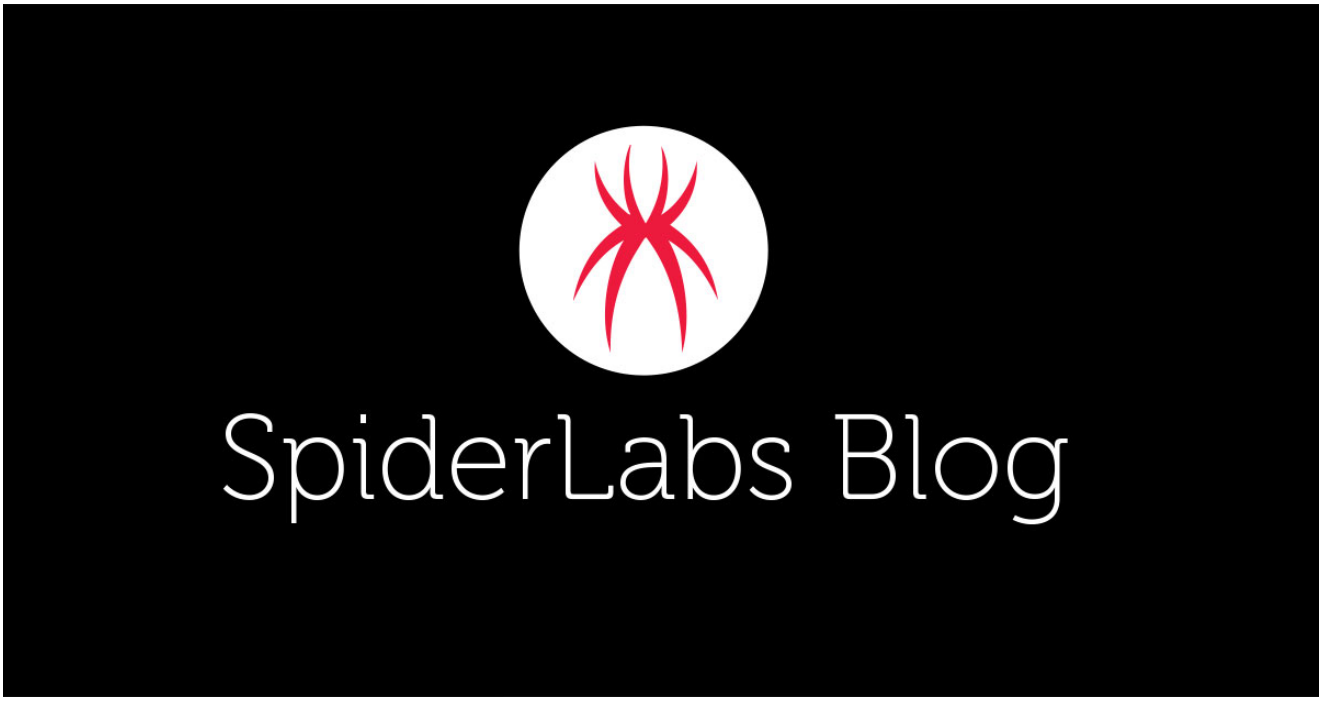
Attacker Tracking Users Seeking Pakistani Passport



A few days ago we encountered a breach on a Pakistani government site which was compromised to deliver a dangerous payload- the Scanbox Framework. This compromise is exactly the kind of attack we were concerned about when discussing the danger in a previous compromise that we uncovered just a few weeks ago against another government site, at that time the Bangladesh Embassy in Cairo.

The compromised Pakistani domain, tracking.dgip.gov[.]pk, is a subdomain of the Directorate General of Immigration & Passport of the Pakistani government that allows passport applicants to track the status of their application. Visitors to the site load the Scanbox javascript code from a remote location. This code collects information about the visitor's machine as well as log any keystrokes the visitor makes while using the site, for example when logging into the tracking system.

In this version that we observed, Scanbox also tried to detect whether the visitor has any of a list of 77 endpoint products installed, most of these are security products, with a few decompression and virtualization tools.

Scanbox Framework is a reconnaissance framework that was first mentioned back in 2014 and has been linked over the years to several different APT groups. Its intense activity during the 2014-2015 years has been well-covered in a paper written by PwC. It was then

seen again in 2017 suspected to be used by the Stone Panda APT group, and once more in 2018 in connection with LuckyMouse.

Scanbox was used in a variety of watering hole attacks, meaning the attacker infected a site with Scanbox in order to gather information about visitors to the site (gathering all the information you'd expect like IP, referrer, OS, User Agent, plugins, etc.) to, later on, tailor sophisticated targeted attacks for interesting visitors. With every appearance, it seems to have evolved in terms of the kinds of information it gathers.

Despite the severity of this infection, scans show an alarming lack of detection for this compromised site by security products:

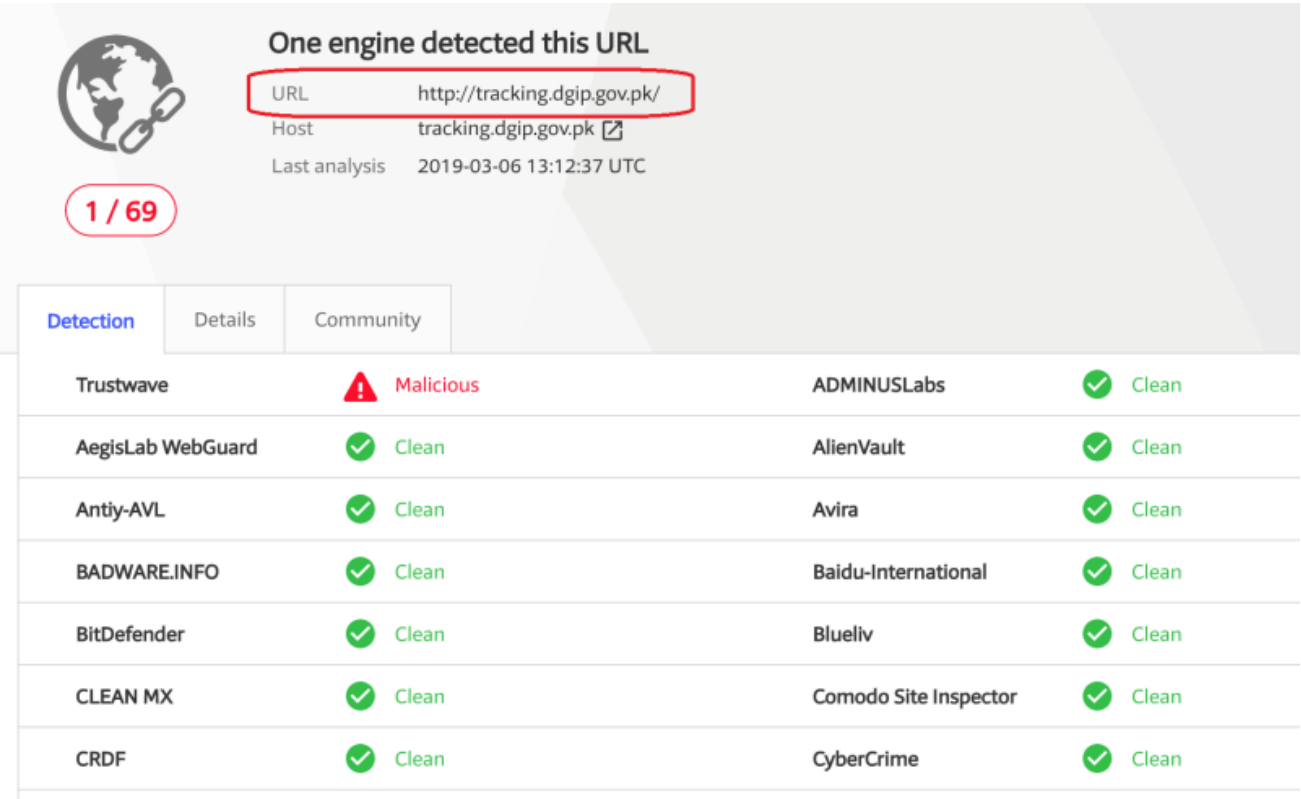


Figure 1: VirusTotal scan results for the compromised URL

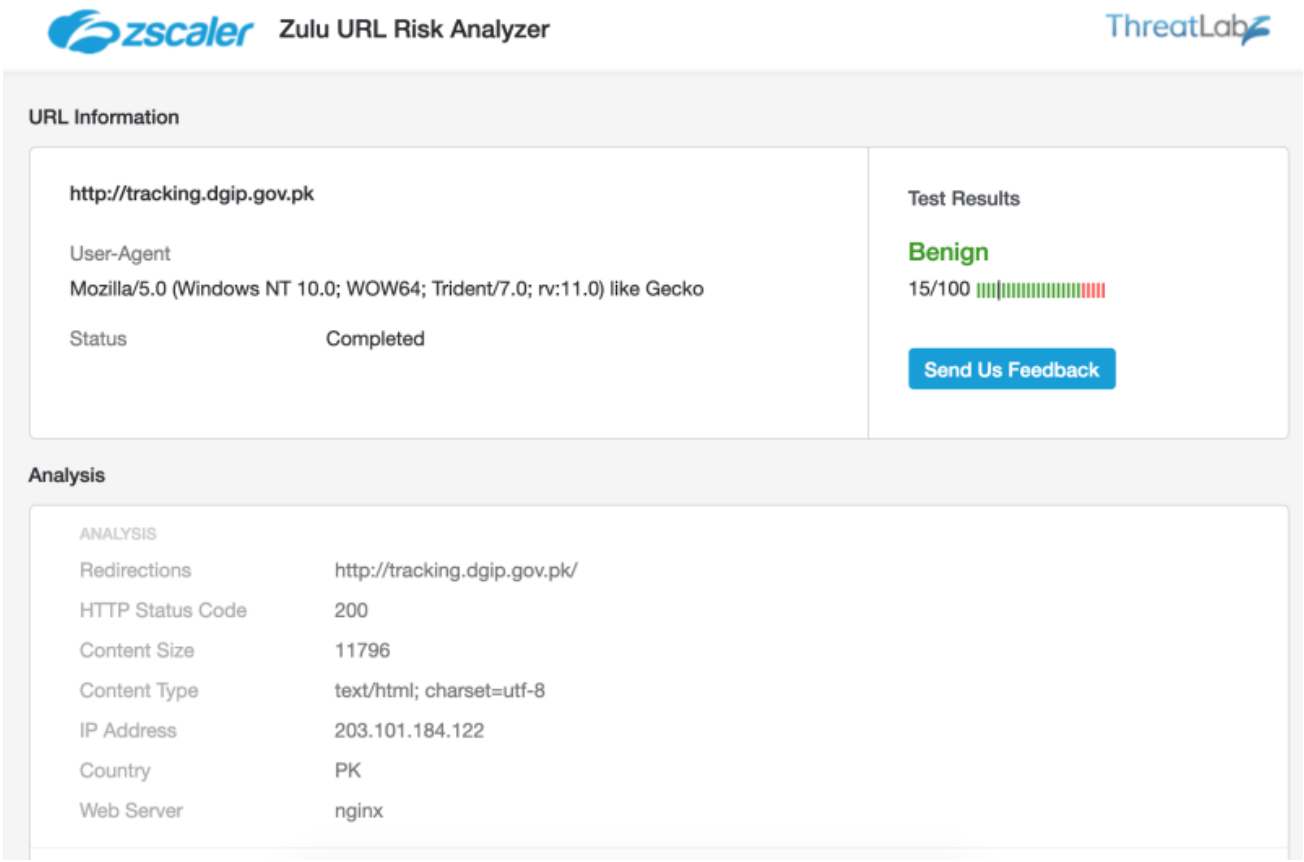


Figure 2: zscaler scan results for the compromised URL

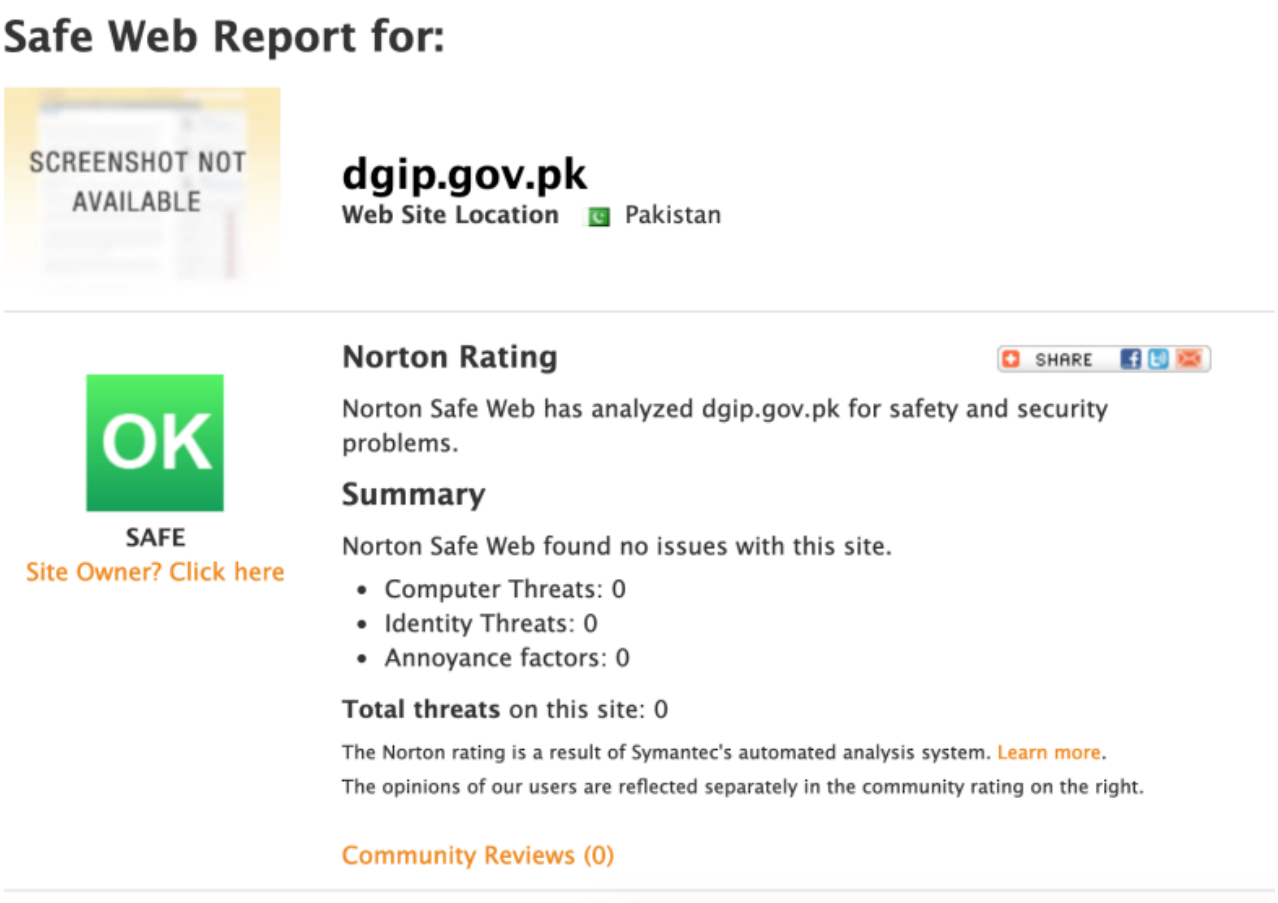


Figure 3: Symantec scan results for the compromised URL

Our earliest detection of Scanbox on this Pakistani government site was on March 2nd, 2019 and though we can't say for sure how long before that Scanbox has been gathering information, we know with certainty that on that day alone Scanbox managed to collect information on at least 70 unique site visitors, about a third of them with recorded credentials.

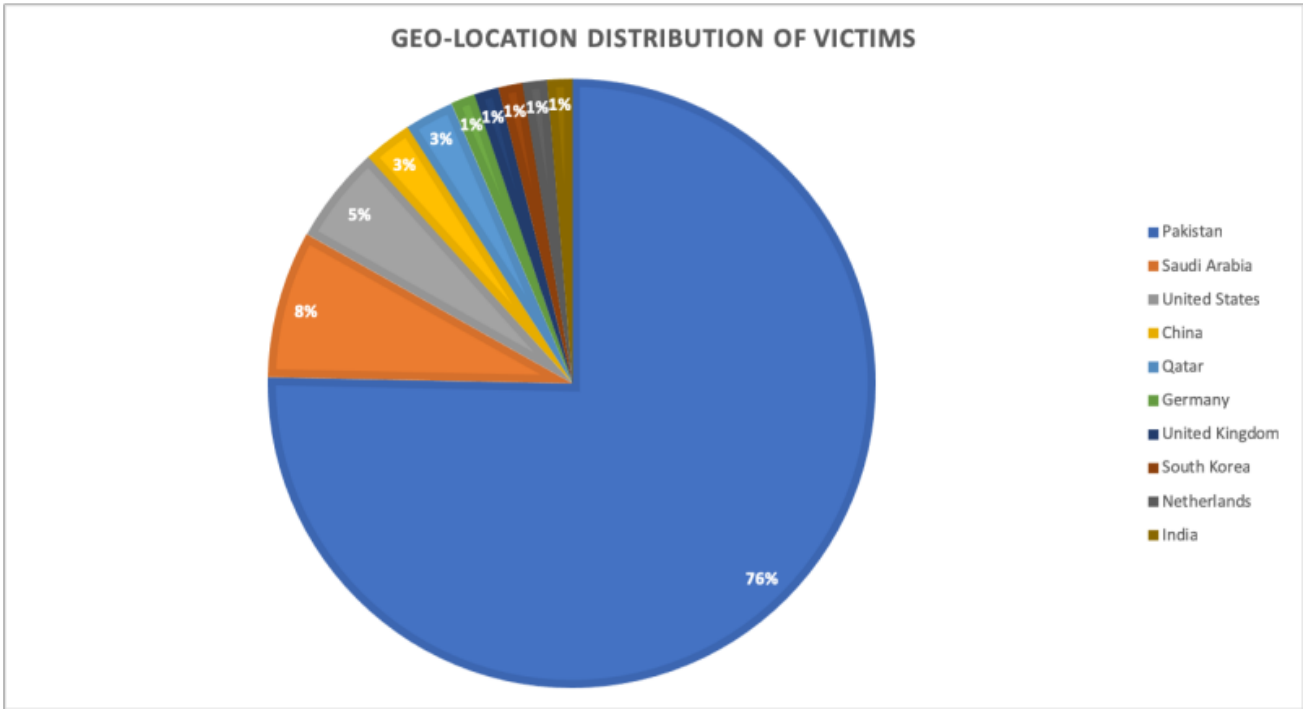


Figure 4: Geo-location distribution of known victims

Shortly after we began our deeper investigation the Scanbox server mysteriously stopped responding, but a VT scan from the time when it was still active shows low detection rates for this server as well:

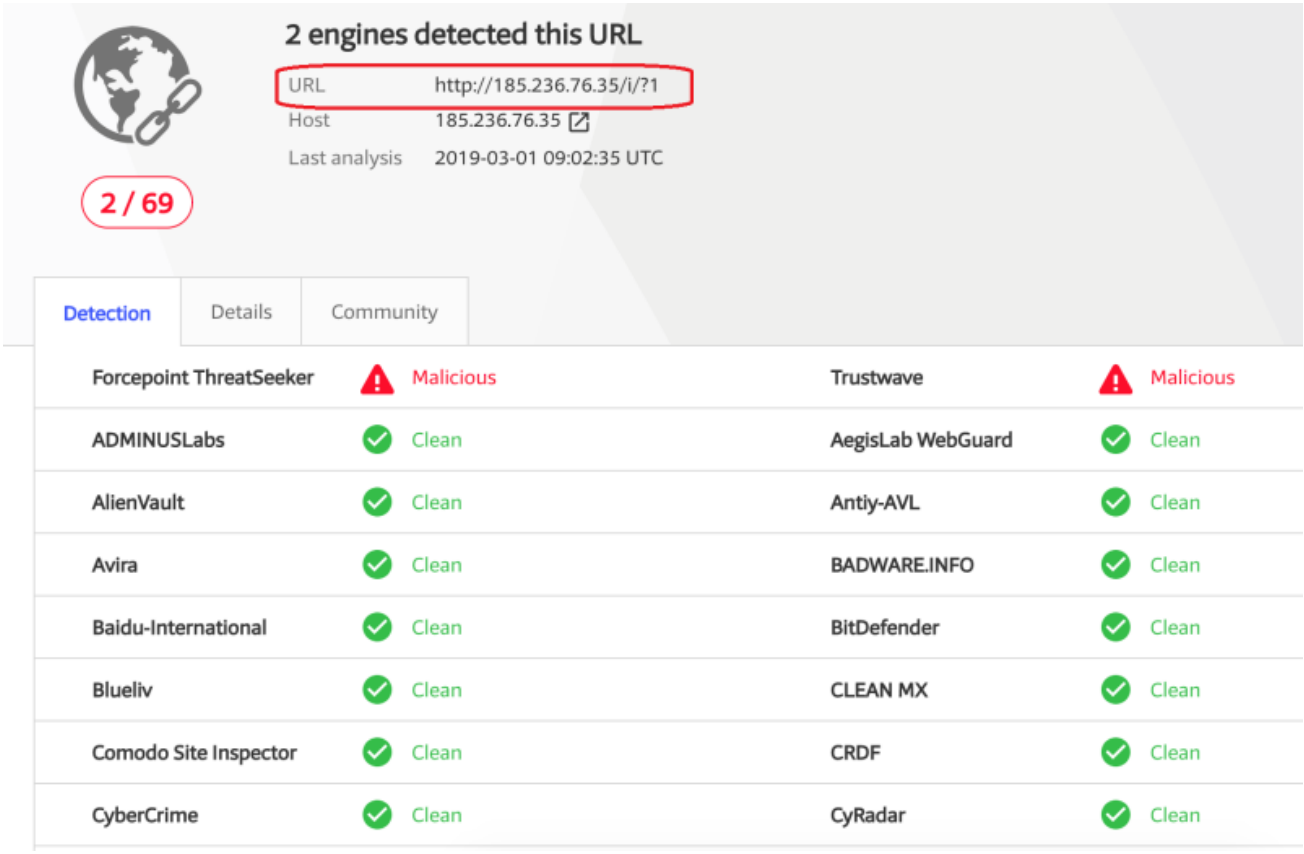


Figure 5: VirusTotal scan results for the Scanbox server

We contacted the Pakistani government site regarding this infection, but as of the time of publishing this blog post have received no response and the site remains compromised. As mentioned above, the Scanbox server currently appears inactive, but the infection indicates that the attack has some level of access to the site, and so it's likely that the server could return to activity or be replaced with a different piece of malicious code at the attacker's will.

These recent cases raise concerns regarding the security of government sites, especially ones where services provided online may involve access to sensitive information. From the perspective of an APT, a tool like Scanbox would only be the beginning of a potentially more elaborate attack.

Trustwave SWG customers are and have been, protected against the Scanbox Framework since 2014 when it first appeared.