EG-CERT

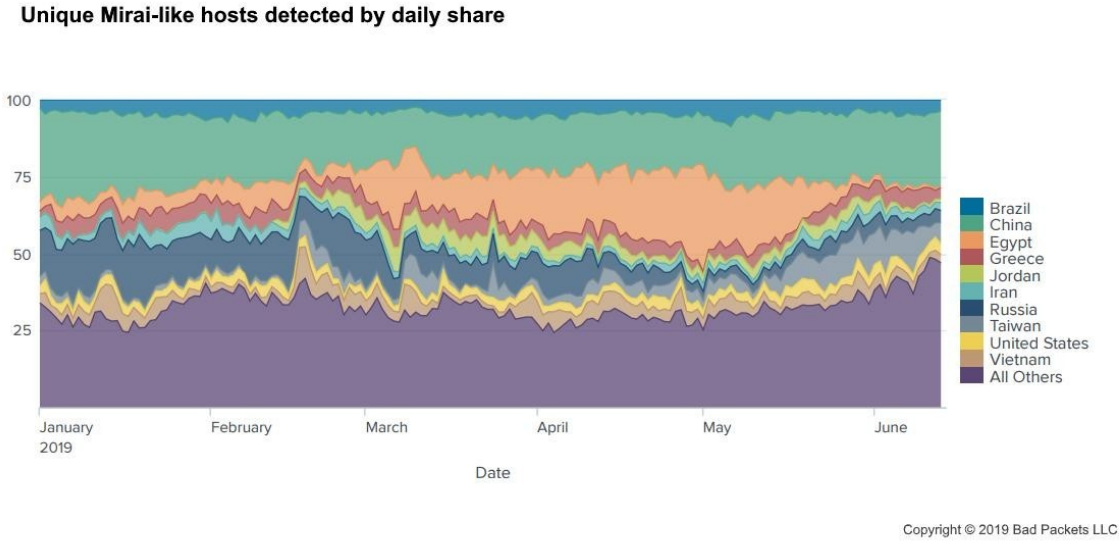
Egyptian Computer
Readiness Team

Alert: Egypt targeted by Mirai-like malware.

Date	18-July-2019
Created By	EG-CERT Malware analysis team

Summary:

- Mirai in a nutshell:
  - "Mirai" is a Linux based malware targeting IoT devices (routers, IP cameras,.. etc) connected to the internet, it scans the internet searching for devices protected by default credentials, then the attacker can use the infected devices to launch a Distributed Denial of Service (DDoS) attack against any target.
  - The source code of the malware was released by its author at the beginning of October 2016, since then many variants of the malware have emerged.
  - The top infection vector is brute forcing a set of usernames and passwords typically set by manufacturer of every device, then the malware is downloaded through telnet or SSH, executed on the device and waits for commands from the C&C server.
- Egypt is one of the most affected targets since January 2019, with more than 20,000 infected hosts, a DDoS attack was launched in March 2019 using these hosts against multiple foreign entities.
- Infected users probably won't notice any change in the service unless there is an active attack similar to the attack that occurred in March.



Source: @Bad_packets

Advisory:

- Perform a factory reset on you router and change your router's default factory credentials, use a private and strong username and password combination.
- Close Telnet service and TCP port 23 of the device.
- If access from the Internet to the device is required, use SSH or other VPN services with strong authentication instead.
- Keep your router's firmware up-to-date to patch any vulnerabilities, contact your service provider to assist you on that matter.