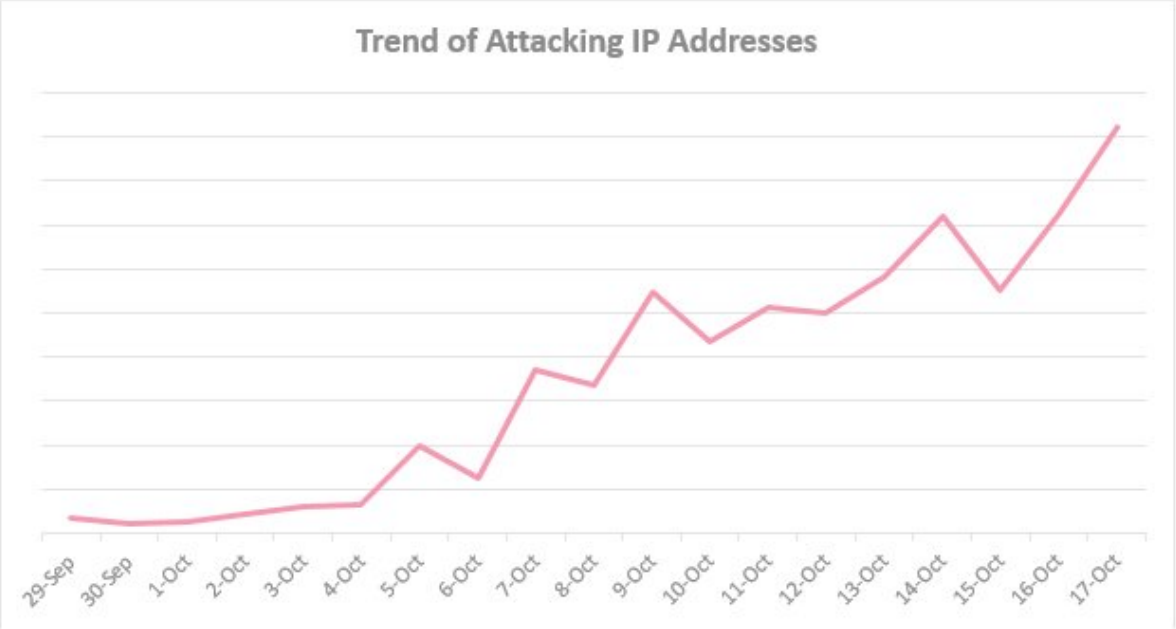
Researchers see gathering of cyber-storm clouds in botnet

October 23 2017, by Nancy Owano



Credit: Check Point Researchers

Security people at Check Point Research have warned us and it is not very pretty. A new Internet of Things botnet storm is in the wings. The team turned up the siren on October 19, warning of a botnet targeting IoT (Internet of Things) devices and saying that it is on the move.

Other tech-watching sites are not in denial.

A massive botnet is forming to create a cyber-storm that could take down the Internet, said Check Point, and an estimated million organizations have already been infected.

The botnet is recruiting devices such as IP wireless cameras to carry this pending nightmare forth. *Wired* referred to it as The Reaper IoT botnet and said it was known alternately as IoT Troop or Reaper. Check Point is calling it IoTroop.

John Leyden, *The Register*, used an army metaphor to explain that it is being assembled, and said it was a "cyber-militia of compromised gadgets." Andy Greenberg in *Wired* called it a "zombie connected-device armies run amuck."

Leyden said the malware has been evolving to exploit vulnerabilities in wireless IP-based cameras, routers, storage boxes, Wi-Fi points, and so on.

What's the motive?

A gruesome ha-ha? Political grudge? Seeking money, or just seeking global attention?

It is too early to assess the intentions of the threat actors, Check Point said.

Numbers, however, seem frightening. Ken Munro of Pen Test Partners was quoted in *The Register*. "We don't know how many have already been compromised, but I've seen comment elsewhere that suggests about 2 million are in a queue to be exploited."

What is a botnet? It is a collection of devices that are Internet-connected.

The devices are infected and controlled by malware. IoT botnets are Internet connected smart devices infected by the same malware and controlled by a threat actor from a remote location, said Check Point. "They have been behind some of the most damaging cyberattacks against organizations worldwide, including hospitals, national transport links, communication companies and political movements."

Who made the discovery?

Wired said researchers at the Chinese security firm Qihoo 360 and the Israeli firm Check Point had details about the new IoT botnet.

HotHardware said, "Researchers at Chinese security firm Qihoo 360 and Israeli outfit Check Point have investigated Reaper and found that it contains millions of potentially vulnerable device IPs, all queued up and ready to be processed by an automatic loader that injects code."

How Check Point took notice: "Our research began at the end of September '17 after noticing an increase in attempts to penetrate our IoT IPS protections. Following this suspicious activity, we soon realized we were witnessing the recruitment stages of a vast IoT Botnet."

The Register described its behavior. The Reaper malware is spreading by exploiting various vulnerabilities in embedded devices, to commandeer them.

Andy Greenberg in *Wired*: "Instead of merely guessing the passwords of the devices it infects, it uses known security flaws in the code of those insecure machines, hacking in with an array of compromise tools and then spreading itself further."

Maya Horowitz, the manager of Check Point's research team, was quoted in *Wired*: "The main differentiator here is that while Mirai was

only exploiting devices with default credentials, this new botnet is exploiting numerous vulnerabilities in different IoT devices. The potential here is even bigger than what Mirai had."

Tech watchers suggested taking various actions.

Leyden in *The Register* suggested (1) to check if you are exposing a vulnerable device to the internet (2) apply any patches if possible (3) watch out for suspicious behavior on your network and (4) take a gadget offline if infected.

"The best thing you can do at the moment is to update any Internet-connected devices you own, and to continue checking for updates," Paul Lilly said in *HotHardware*.