Kateryna Veryha
M. S. Dushenok, language advisor
I. A. Golubova, research supervisor
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”
Educational-Scientific Complex “Institute for applied system analysis”

IoT Botnets Analysis

A botnet is a set of connected devices which have been infected with malware that allows an attacker to gain remote control and coordinate their actions. Attackers most commonly use their botnets to launch DDoS (Distributed Denial of Service) attacks but they can also be used to send spam emails, sniff out sensitive passwords, or spread ransomware.

The Internet of Things (IoT) is the name given to describe relatively new technology that connects everyday objects and devices to the web to provide additional data or functionality.

Botnet is not a new concept, but previously it commonly meant a big controlled amount of infected PCs, so several techniques to prevent infection with malware are well-known. And vice versa, devices in IoT are quite new and not standardized completely and, as a result, do not have effective enough security protocols to withstand infiltration. Recent DDoS attacks, with hundreds or even thousands of devices, all with their own unique IP addresses, a hacker makes it almost impossible to stop the attack. While, at this point, IoT botnets have primarily been used by low-level actors for the purpose demonstrating their capabilities or testing out the tool, it is only a matter of time before cybercriminals and hacktivist groups adopt the tactic to carry out politically or financially motivated large-scale attacks.

As more organisations become dependent on Internet connectivity, data and application services for day-to-day business continuity DDoS represents significant risk. This is being addressed by many businesses and more than half enterprises are now factoring the DDoS threat into their business risk management processes, so that it gets the right focus.

Attackers will likely invest more resources into taking over the hordes of IoT devices added to the Internet every day. Device manufacturers need to use the recent attacks as a wakeup call to refocus on securing their products. At a minimum, manufacturers should remove unnecessary network services and include ways to easily or automatically patch security vulnerabilities in their products.

IoT consumers should treat their devices similarly to their personal computers when it comes to security best practices. It will take a combined effort of manufacturers and consumers to slow the spread of IoT botnet malware, but it is possible.