1. Summary Article
   1. Summary: This article gives a general definition of botnets as: ”Botnets are networks of computers infected by a botnet agent that are under hidden control of a third party. They are used to execute various commands ordered by the attacker. Most common uses of botnets are criminal operations that require distributed resources, such as DDoS attacks on selected targets, spam campaigns, and performing click fraud. Often, the botnet agent is ordered to download and install additional payloads or to steal data from the local computer.” They also state that the first botnet appeared around 1999 (this number seems to shift slightly based on the site),
   2. Key Points:
      1. Bots need a C&C.
      2. Typically used for DDoS attacks.
      3. Neutrino: focuses on performing various types of DDoS attacks and stealing data from infected computers
   3. Link: <https://blog.malwarebytes.com/threats/botnets/>
2. Summary Article
3. Summary: This article defines botnets as: “the generic name given to any collection of compromised PCs controlled by an attacker remotely. Botnets generally are created by a specific attacker or small group of attackers using one piece of malware to infect a large number of machines. The individual PCs that are part of a botnet often are called “bots” or “zombies” and there is no minimum size for a group of PCs to be called a botnet. Smaller botnets can be in the hundreds or low thousands of infected machines, while larger ones can run into the millions of PCs.” It also includes some common infection methods, such as browser vulnerabilities, email infections, and word or pdf infections.
4. Key Points:
   1. Infection points include browser vulnerabilities, email infections, and word or pdf infections.
   2. Well known examples are: Conficker, Zeus, Waledac, Mariposa and Kelihos.
   3. Botnets are also used to send junk mail.
5. Link: <https://blog.kaspersky.com/botnet/1742/>
6. Specialized Article
   1. Summary: Missing passwords, and lack of encryption: Weak and absent passwords are both common on the internet, and specifically a problem with IoT. Poorly designed IoT devices also lack encrypted communications, which opens up a couple of major issues. One, sensitive personal information is transmitted in the clear, for anyone on the local network and upstream network to eavesdrop on. And two, IoT devices cannot be sure they're communicating with the real and correct vendor-supplied web applications or mobile apps. Encryption isn't just about keeping secrets, it's also about authentication, so an IoT device that operates in cleartext, rather than over encrypted channels, is inherently untrustworthy.
   2. Key Points:
      1. Need stronger passwords
      2. Need better encryption methods
   3. Link: <https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html>
7. Specialized Article
   1. Summary: While DDoS attacks from Mirai botnets can be mitigated, there’s no way to avoid being targeted. However, as a device owner, there are things you can do to make the digital space safer for your fellow Internet citizens:
   2. Stop using default/generic passwords.
   3. Disable all remote (WAN) access to your devices. To verify that your device is not open to remote access, you can use this tool to scan the following ports: SSH (22), Telnet (23) and HTTP/HTTPS (80/443).
   4. With over a quarter billion CCTV cameras around the world alone, as well as the continued growth of other IoT devices, basic security practices like these should become the new norm. Make no mistake; Mirai is neither the first nor the last malware to take advantage of lackluster security practices.
   5. Link: <http://www.techrepublic.com/article/security-experts-whats-wrong-with-internet-of-things-security-and-how-to-fix-it/>
8. Specialized Article
   1. Summary: Many devices have security issues that come from the manufacture “Devices usually contained a system on a chip (SoC) that executed the actual protocol connection to the internet. Vulnerable devices also had active login passwords that had not been changed from the default settings. Since the chip was integrated into some other product, the user may not have been offered the option to change the login info — perhaps the manufacturer found these default credentials useful in testing the overall device. However, these default passwords gave the attackers the elevated privileges they needed to carry out their criminal campaigns.”
   2. Key Points:
      1. Check open ports.
      2. Disable protocols that aren’t needed.
   3. Link: <https://securityintelligence.com/the-internet-of-trouble-securing-vulnerable-iot-devices/>