The Internet of Things (IoT) is a relatively new network of Internet-enabled everyday objects (e.g., "smart" lightbulbs, thermostats, doorbells, etc.) that have seen explosive growth with no sign of stopping. IDC forecasts worldwide IoT spending will surpass the $1T mark in 2022. IoT devices are an increasingly common tool for massively destructive attacks.

Mirai and the Botnet of Things

In 2016, attackers used an IoT botnet to launch, what was at that time, the largest recorded DDoS attack at service provider Dyn. The attack subsequently took out many popular user services, including GitHub, Twitter, and Netflix.

The IoT botnet was a result of Mirai, malware that targeted vulnerable devices and used a list of known default usernames and passwords in attempts to gain access. If the owner of the device never changed its default credentials, Mirai was able to log in and take over.

Vulnerability Exploits

Vulnerability Exploits

IoT devices, limited by their size and processing power, typically use a lightweight protocol for communication such as CoAP. However, this machine-to-machine protocol is vulnerable to IP address spoofing and packet amplification.

Reflective Amplification Attacks

Whereas PC security has improved over the years, IoT devices often still suffer from rudimentary vulnerabilities that attackers can easily exploit. In many cases, patches for these pitfalls cannot be deployed remotely, leaving an entire generation of machines and their users vulnerable.

Incorporate DNS Security

Incorporate DNS Security

Domain Name System (DNS) is the entry point for every Internet-connected device and application, enabling devices to connect, discover, and communicate. Farsight collects Passive DNS data from its global sensor array and then filters and verifies the DNS transactions before inserting them into the DNSDB along with ICANN-sponsored zone file access download data. The result is the highest-quality and most comprehensive Passive DNS data service of its kind. DNSDB is engineered and operated by leading Farsight DNS experts.

Using DNSDB, organizations can derive meaningful insights to drive actions such as:

• Connect attacks to specific domains, IPs, ASNs, and email addresses to map out malicious infrastructure
• Detect suspicious spikes in global DNS queries for a specific domain
• Predict future attacks by identifying related domains and IPs associated with malware