bugcrowd

IOT SECURITY

Your Brief on the IoT Threat Landscape

We are on the verge of a major technological revolution: interconnectivity at scale, anytime and anywhere. IoT has paved the way for smart cities, improved productivity, the connected home, and ultimately more opportunities to connect with one another.

To date, IoT has gone unregulated and largely unsecured, and given the rapid growth of IoT devices it's no surprise that these devices represent a growing security threat. The sheer number and types of the devices being networked and connected to cloud interfaces and on-the-internet APIs is one the greatest challenges in security today. Each device has its own set of technologies, thus its own set of security vulnerabilities.

IoT Vulnerability Landscape

Year over year, we see a significant increase of IoT vulnerability submissions — **383.6%.**

The majority of the vulnerability submissions fall in the P3 level of criticality, just over **35%.**

Total payouts in Q1 2019 increased by **88.6%** compared to Q1 2018.

The average payout for Q1 2019 was **$2,318.61** per vulnerability — **78%** year-on-year.

The average payout for P1s in Q1 2019 is **$8,555.56**, which is higher than any other year combined.

More than **14%** of all IoT submissions are classified as P1 submissions, the most critical vulnerabilities.

Security is a growing concern around the world. Today nearly every person has been impacted (148 million Americans had personal data compromised in the 2017 Equifax breach alone). And with a large and growing number (3.5 million) of unfilled cybersecurity jobs organizations and government agencies around the world are struggling to keep up.

IoT Stats & Hacks

1. Experts predict that **by 2025, there will be as many as 75 billion connected IoT devices.**
2. Mozilla mentions there will be up to **30 billion connected devices** by 2020.
3. In October of 2016, **the largest DDoS attack ever was launched on service provider Dyn** using an IoT botnet. This lead to huge portions of the internet going down.
4. Early last year, **CNN** wrote, "The FDA confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities that could allow a hacker to access a device.
5. Right behind the St. Jude cardiac devices is the **Owlet WiFi baby heart monitor.**
6. Kaspersky Lab suggests **people should be especially on alert for malware attacks** related to their IoT devices. The research team found **a threefold increase** in the malware attacking smart gadgets last year.

> "The IoT is going to power our ability to ask important, human-focused questions of our environment--and to get continuously-updated answers to those questions. And if we don't have security baked into every layer of that stack, a flaw at any level could undermine the entire thing—with human, not just technical—consequences." **Daniel Miessler, OWASP IoT security project lead**

The number of IoT-focused programs on the Bugcrowd platform is growing. Today we work with Fitbit, Arlo, NETGEAR, Tesla, Fiat Chrysler Automobiles, HP, Samsung, Cisco Meraki, as well as a number of others.

Learn why IoT industry leaders have turned to Bugcrowd

bugcrowd.com/get-started