Rajat Sethi

CPSC 8580

**Paper Summary – IoT Malware Lifecycle**

The Internet of Things (IoT) is a relatively new subject in the field of computer science. Manufacturers all over the world are making their devices “smart” by connecting them to the internet and issuing commands using human voices. Unfortunately, due to the novelty of IoT devices, a flood of viruses, botnets, and malwares have infected these systems and networks. This paper takes a closer look at the nature of these malware, analyzing how they penetrate devices, avoid detection, cause damage, and spread.

The key novelty of this paper is its conglomeration of data. The paper claims to have analyzed over 166,000 IoT “supplies” for vulnerabilities and malwares. Using a combination of ELF/Executable/Binary analyses (static) and network traffic analyses (dynamic), the research team was able to determine several methodologies that IoT Malwares exploit to achieve their malicious goals. This ranges from cross-checking multiple anti-virus engines, utilizing a honeypot to attract hackers, studying the polymorphism and evasion techniques of modern malware, and analyzing the ways that malwares siphon data or cause damage in a persistent manner.

The greatest limitation of this paper was its lack of code or technical examples. The researchers would mention a vulnerability label like “Mirai” or “gafgyt,” but then they would not explain how the malwares worked from a coding perspective. They would also mention a few files located in the root system, but not the actual contents of those files that could be attacked by malware. What commands were the malware using? What specific ports or programs were being targeted and why were they so easy to attack? Overall, this paper felt more like a summary of things that IoT malware has done, but not a paper of how its done.

In future works, I sincerely hope this paper goes into more depth about the actual malware they are trying to analyze. They have the full capabilities of analyzing what the attack was and what general method was taken, but they should also try and be more specific as to what code snippets were used in the attack. On another note, the researchers should also consider explaining the relevance of their related works. More often that not, they would paste some jargon with a reference, but would not elaborate on what the jargon meant. It was as if they expected us to read all 70 papers found in the bibliography. I would sincerely hope that in the follow-up to this paper, the jargon is superficially explained so that it can remain relevant to the article.