The usage of Internet of Things (IoT) devices is growing fast. Moreover, the lack of security measures among the IoT devices and their persistent online connection give adversaries an opportunity to exploit them for multiple types of attacks, such as distributed denial-of-service (DDoS). To understand the risks of IoT devices, we analyze IoT malware from an endpoint standpoint. We investigate the relationship between endpoints infected and attacked by IoT malware, and gain insights into the underlying dynamics in the malware ecosystem. We observe the affinities and different patterns among endpoints. Towards this, we reverse-engineer 2,423 IoT malware samples and extract IP addresses from them. We further gather information about these endpoints from Internet-wide scans. For masked IP addresses, we examine their network distribution, with networks accumulating more than 100 million endpoints. Moreover, we conduct a network penetration analysis, leveraging information such as active ports, vulnerabilities, and organizations. We discover the possibility of ports being an entry point of attack and observe the low presence of vulnerable services in dropzones. Our analysis shows the tolerance of organizations towards endpoints with malicious intent. To understand the dependencies among malware, we highlight dropzone characteristics including spatial, network, and organizational affinities. Towards the analysis of dropzones' interdependencies and dynamics, we identify dropzones chains. In particular, we identify 56 unique chains, which unveil coordination among different malware families. Our further analysis of chains suggests a centrality-based defense and monitoring mechanism to limit malware propagation. Finally, we propose a defense based on the observed measures, such as the blocked/blacklisted IP addresses or ports. In particular, we investigate network-level and country-level defenses, by blocking a list of ports that are not commonly used by benign applications, and study the underlying issues and possible solutions of such a defense.