In the digital age, the world has become more connected than ever. Technologies like artificial intelligence, machine learning and internet of things (IoT) are making inroads into industries, offices and now even homes. As per recent Gartner estimates, there will be 6.4 billion connected things globally by the end of 2019 and this is expected to increase to 21 billion by 2020. While the benefits of a connected ecosystem are undeniable, the risks involved in such an ecosystem can also not be overlooked.

The prime concern is security as IoT devices installed in offices, factories and homes are vulnerable to malware attacks. In an increasingly connected world, malware can easily travel from one device to another and even to a larger host network. According to a survey conducted by ForeScout, businesses are not yet prepared to manage IoT devices and 85 per cent of the 350 IT professionals surveyed by the company stated that they were not sure if they could detect an infected IoT device as soon as it connects to the network. Despite the growing instances of IoT-originated malware attacks, the industry remains largely unprepared.

A look at the recent instances of malware attacks on IoT devices, the consequences of such attacks and how they can be prevented...

Increase in malware attacks

In recent years, the industry's fears regarding IoT device security have been legitimised. In October 2016, a series of distributed denial-of-services (DDoS) attacks was launched on DNS service provider Dyn, infecting it with the Mirai malware. This was the first large IoT malware attack that caused significant losses. Through this malware, the hackers breached thousands of IoT devices such as IP cameras, baby monitors and network printers, and infiltrated the Twitter, Visa, Netflix and Reddit accounts of DYN's customers.

In April 2017, another IoT malware called BrickerBot crept into several thousands of IoT devices and bricked them by overwriting the stock firmware with some random code. In 2018, VPNFilter malware was introduced by malicious actors. The malware is designed to infect routers and storage devices. One notable feature of this malware is that it can survive even after the infected device is formatted. Moreover, VPNFilter malware is capable of carrying out multiple payloads that can steal valuable credentials from the host system, capture and erase all data, among other such things.

The number of IoT attacks has increased significantly. As per a recent analysis by security firm F-Secure, the number of IoT threats doubled between 2017 and 2018, growing from 19 to 38 in a span of one year. According to Symantec's global analysis of IoT attacks, around 5,200 IoT attacks per month were reported on an average throughout 2018.

The most common strategy deployed by these attackers is the use of botnets. As part of this, the attackers take control over thousands of vulnerable IoT devices and turn them into a network of botnets to carry out DDoS attacks by sending out a stream of network requests to the targeted server or computer network. Further, most attackers exploit loose ends such as unpatched software, weak or default passwords, or a combination of the two. According to a report by F-Secure, these access points account for around 87 per cent of the observed threats.

Origins and consequences

Due to the increasing penetration of IoT devices, there is now a greater threat of cyberattacks. As IoT adoption moves beyond industry use cases, and deeper into the day-to-day lives of people in the form of smart homes, smart cars, etc., the risk points involved have increased manyfold. This includes valuable data of organisations and individuals, their financial information, personal information and client sensitive information.

An increasingly connected ecosystem offers numerous entry points for a malware attack. As per Symantec's analysis, infected routers were the source of 75 per cent of the attacks carried out in 2018, while connected cameras were the source of 15.2 per cent of such attacks. The study noted that the number of attacks carried out through connected cameras has increased significantly from 3.5 per cent in 2017 to 15.2 per cent in 2018. In the enterprise realm, anything and everything works as a favourable access point for malware. It can be introduced through printers installed at offices, CCTV cameras, employees' computers, and even through a central temperature controlling system. According to a February 2019 Avast report, the biggest IoT threats to businesses come from security systems such as cameras and doorbells, which record sensitive company data. According to a Gartner IoT Security Survey Report 2018, most organisations already face information risks from IoT devices and almost 20 per cent of organisations have detected an IoT-based attack in the past three years.

Once a malware creeps into the network, its consequences can be disastrous. As per the State of IoT Security Survey 2018, 25 per cent of the companies struggling with IoT security-related issues, reported cumulative losses of at least $34 million in the past two years. While the monetary loss incurred due to breach in systems is significant, it is not the only kind of financial loss caused by a malware attack. As per industry reports, organisations can potentially lose millions of dollars because of the downtime caused by attacks on their IoT devices and networks. In addition to the monetary loss, such malware attacks even jeopardise the reputation of a company and affect the volume of the company’s business in the long run.

Solutions and the way forward

The lack of standardisation and strict regulations is one of the reasons of these attacks as it allows vendors to follow poor security practices while developing their products. Vendors often launch poorly developed devices in the race to be the first in the market. Such devices are quite vulnerable and ill prepared to sustain any malware attack even before they are installed at offices and connected to the larger network of the organisation.

Thus, it is essential that the testing of devices is moved to the earlier stages in the entire process. Organisations can deploy white-box testing methods such as static application security testing, which allows businesses to keep a check on the infiltration of the devices on a continuous basis. It also enables developers to identify the weak links in the code at the start, thereby putting them in a better position to address these vulnerabilities. The continuous testing approach enables developers to analyse the changes introduced to the code on a regular basis. Developers are notified if any vulnerability is found, providing businesses with enough time and information to take preemptive action.

The security-by-design approach suggested by Deloitte involves incorporating cybersecurity practices by default into the product’s design as well as into the environment in which it is implemented. This helps organisations save time and reduces costs by fixing security issues during the initial phases of product development.

While big firms like Google, Amazon and Apple have taken considerable steps to make their smart product offerings more secure and protected against cyberattacks, the larger industry comprising many small players is still lagging behind. Going forward, it is essential that the industry as a whole develops and adopts benchmark security practices.

About Us We are Hiring Contact Us

Subscribe Privacy Policy Advertise Terms & Conditions