The use of insecure IoT devices in the creation and propagation of criminal distributed systems(botnets) and the implications of these bots on their local networks.

UP877962 | MEng Computer Science

Abstract

The IoT (internet of things) is the name given to the growing number of internet connected devices that gather data from, allow the control of a device or share data, often over the internet. The number of these devices in use is rising exponentially however the efforts to ensure they are secure are not following the same pace. (***Leuth, K.L. 2018***)

The paper aims to look at the way IoT devices are being compromised at both the network and device level for the purposes of being recruited into botnets and then used to carry out malicious activities on behalf the of the botnet owner, in particular this paper focuses on the effects a compromised device can have on its local network.

The paper looks at the ways these compromised devices can be used to cause damage, disruption and potentially lead to further devices being compromised on an internal distributed system and what can be done to mitigate this happening.

Introduction

Many current IoT devices are inherently vulnerable due to a number of factors such as being shipped with generic passwords or lack of security patches when vulnerabilities with the system are uncovered, there has been a major rush to bring these products to market but unfortunately this has not been matched by a desire to ensure these products are secure (***M. M. Hossain, M. Fotouhi and R. Hasan, section 2 2015***).

With the number of IoT devices connected to the internet growing exponentially and the total expected number of connected devices expected to hit approximately 75 billion devices by 2025, up from roughly 15 billion devices in 2015(***statista 2019***) there is a clear need to ensure that these devices are not being used maliciously.

The Mirai malware and its many variants specifically target IoT devices and commonly consist of two distinct components. There is a scanning element that searches the internet for poorly secured devices and brute forces its way onto these devices and reports back system information to the botnet controller and then an attack element that delivers the payload to the insecure device, these payloads often contain malicious code designed to take advantage of vulnerabilities in the device to gain complete control of it and in turn access to its local network (***Kolias, C et al.. 2017***).

This paper aims to explore the potential harm that can be caused by compromised devices on a local network, and in a commercial/industrial setting where there may be many of these devices controlling machines or acting as servers etc.

Problem statement/aim and objectives

The problem being explored is the use of insecure IoT devices in the creation of botnets and the vulnerabilities that these expose at both the network and local level once compromised, this is a problem that is only going to become more prevalent and damaging the more of these devices there are especially as in some local environments there are often many of these devices connected in their own internal distributed system (***K. Iwanicki 2018***). The aim is to identify solutions and best practices when designing and deploying these devices. The experiment aims to showcase some current vulnerabilities and their effects on various devices on an internal distributed network when one IoT device has been compromised and then aims to gather enough information about these vulnerabilities to be able to formulate a solution to mitigate these vulnerabilities.

Background

There are many malware (malicious software) that are aimed specifically at IoT devices that allow the attacker to force infected devices to carry out amongst other things sending spam emails, DDoS attacks, cryptocurrency mining or attacking the network the infected device sits within, in fact as computer manufacturers improve the security of their devices the creators of these botnets are increasingly switching to softer targets (***N Forrester 2020***).

The Mirai malware in particular is one that has had enormous impact in recent years such as a 2016 attack on dynDNS, a DNS naming service and part of the backbone of the internet that caused major outages across north America and Europe and is considered one the largest DDoS ever seen. (***J Fruhlinger 2018***) This is just one example of the many different malware and although very effective Mirai relies almost entirely on generic or easy to guess passwords in order to gain access to a device. It is estimated that by 2030, 25% of all cyberattacks will involve IoT devices and malware is constantly being refined so a proactive approach is required (***Nguyen, H., Ngo, Q. & Le, V 2019***).

One study that was carried out by chance after the authors were carrying out an experiment designed to catch other malware shows the true scale and spread of these systems and in particular the way this one in particular didn't target personal computers but IoT devices.

Figure 1 (image showing the scale of live devices on the botnet)

This particular botnet was using the P2P protocol which makes it harder to take down, however made it easier for the authors to track the size of it by decoding the traffic and then injecting their own command's into the system using man in the middle attacks. The network was showing roughly 8300 live devices per day (see figure 1) of which around 45% were raspberry pi SBC (single board computers) often used as headless servers for a variety of purposes and also for many IoT projects with a further 21% running the openELEC platform, a media server platform often run on raspberry pi's and other similar devices. The rest of the botnet consisted of compromised wireless access points and storage devices. (***Marinho, R. 2017***)

Experimental design

For this experiment the aim was to simulate an internal distributed system consisting of many different devices (see figure 2) where one individual IoT component has been compromised, an ESP8266 microcontroller that costs around $3 although this could potentially be any IoT device (the more powerful the device the more damaging the attacks that could be launched) and then used against other components of the system to create an internal DDOS attack across many devices showcasing how an entire system can be compromised by one of these devices. In a business setting this could potentially be disastrous and in fact while researching for this experiment over 50 esp8266 with vulnerabilities including readable credentials were found on the Shodan IoT browser, incredibly, many of these were with telecoms companies around the world. (***Shodan. 2020***) The ESP8266 has been loaded with a legal wi-fi de-authentication firmware package that can be installed over the air, this could also be written as a script on the device in many different languages and without the limitations of this legal version. The software pairs to a smartphone over http to scan and launch attacks on local networks and includes de-authentication, broadcast and probe elements allowing spoofing of access points and gaining in depth information about the network and devices attached to it. (***Spacehuhn. c2020***)

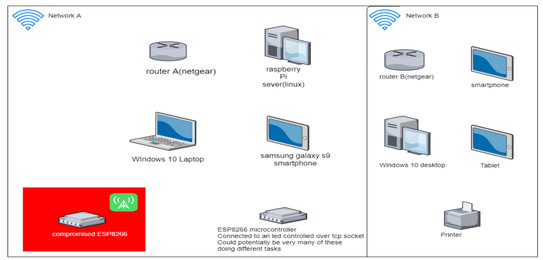

Figure 2, The devices and networks used are shown above

Results

The results were analysed by testing each network as a whole and then individual devices on the networks starting at the routers then moving down to individual devices, the results are as follows:

Network 1- ESP8366, windows 10 laptop, and raspberry pi server forced offline (limitation with de-authenticator or it would have been all devices on network). All access points on the network spoofed. No internet access on affected devices, TCP socket connection between Samsung phone and the test LED on the 2nd ESP8266 failed. On the 2nd run Router A, Samsung galaxy phone, and ESP8266 forced offline. Router A's SSID spoofed, Internet connections and TCP sockets disabled. Successful denial of service over the network. Password prompt on spoofed access points.

Router A – targeted individually, successful DOS and spoofing of SSID
Raspberry Pi server - targeted individually, successful DOS and spoofing of SSID
Windows 10 laptop - targeted individually, successful DOS and spoofing of SSID
Samsung galaxy s9 - targeted individually, successful DOS and spoofing of SSID
ESP8266 - targeted individually, successful DOS and spoofing of SSID

Network 2 – Printer, and windows 10 desktop forced offline, the router itself was unaffected as well as a tablet computer and mobile phone. All the SSIDS were spoofed.

Router A – targeted individually, unsuccessful DOS and successful spoofing of SSID
Windows 10 desktop - targeted individually, successful DOS and spoofing of SSID
Printer - targeted individually, successful DOS and spoofing of SSID
Smartphone - unsuccessful DOS and successful spoofing of SSID
Tablet computer - unsuccessful DOS and successful spoofing of SSID

Discussion

The results of this experiment were not what was expected before carrying it out, the expectation was to have limited access to some elements of the network such as Linux servers and other microcontrollers, however being able to affect a smartphone and windows pc was surprising.

The probe attack was not used as part of the experiment, however this could have been used to gain further access to other devices by capturing handshakes and using brute force attacks on the password, however the point of the experiment was not to demonstrate hacking but to show how inherently vulnerable these devices can be, and as users including commercial and industrial users rush to incorporate more of these types of devices into their networks the threat and risk is going to rise exponentially (***Forrester, N. 2020***).

Take for example the 2nd ESP8266 microcontroller used in the experiment, this was set up to receive commands via TCP over the local network, if this was a machine in an industrial setting that was prevented receiving an on/off command this could lead to damage to the machine itself or further implications for the rest of the production system, or if the server or router were targeted this could give attackers complete access to the entire system.

The decision to use the ESP8266 microcontroller was based on nothing but availability, however these microcontrollers are mass produced, widely used and very cheaply available at around $3 per device. The microcontroller uses a RISC processor and instruction set that are widely used in IoT devices including in ARM processors and are actively being targeted by botnets, including variants of the Mirai malware. (***Kolias C, et al.. 2017***) With the number of these types of devices growing exponentially and being used for more and more diverse roles, the attack surface and desire to attack such devices will also grow.

One of the biggest factor with this type of attack is the lack of mass adoption of the wireless 802.11w standard, which provides encryption for the management frames that were interrupted by this attack and in fact this is very often the first part of attempts to carry out more malicious activities on the network, the standard requires that both devices have it enabled and this was the case with the router and 2 other devices on the 2nd network however the first network was completely unprotected.

Conclusions

There are already many solutions available that can help to mitigate the risk of IoT devices being compromised, however they are not being adopted in a widespread manner. The 802.11w standard being an obvious solution that was introduced in 2009 and encrypts management frames yet is not incorporated even in modern (less than 2 years old) devices, this one simple move would prevent de-authentication attacks and also protect the handshakes from being picked up by probe attacks thus paving the way for further attempts on the network, with these being common ways of launching attacks on networks and recruiting new devices to botnets.

Newer architectures may also offer a solution with these devices often very basic and low powered making them unable to run a feasible software solution, RISC-V for example offers the opportunity to increase security on these types of devices at the hardware level by allowing modularity in the way they are designed enabling developers to exclude unnecessary instructions and including new cryptographic mechanisms (***Speers, T. 2019***).

The way the devices are configured needs to be scrutinised, another search of the Shodan IoT web browser showed 160 ESP8266's with open outward facing interfaces and some also showing credentials, considering this is just one type of hardware out of many thousands more similar IoT devices there are huge numbers of insecure IoT devices open to attack , earlier versions of the Mirai botnet relied on scanning for available IP addresses and a password dictionary of less than 100 common passwords however managed to infect many thousands of devices globally (***Kolias C, et al.. 2017***).

There is a need for a global standard for IoT devices, at present these devices are being produced extremely cheaply and are being used more and more in all manner of settings, but there is no regulation of the devices security, confidentiality, integrity or availability.

Future work

There is a need for the implementation of a global standard for IoT devices to prevent these devices being recruited to botnets and/or used maliciously on internal distributed networks to cause damage, disruption or to gain access to systems and data on the network. The next step in the research on this project would be to look further at existing and emerging technologies that can be implemented into a recognised standard for IoT devices and then to present these findings in their own context.

References

Leuth, K.L. (2018). State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. Retrieved 24 March, 2020, from https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

M. M. Hossain, M. Fotouhi and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," 2015 IEEE World Congress on Services, New York, NY, 2015, pp. 21-28.

Statista. (2019). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). Retrieved 24 March, 2020, from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Kolias C, et al.. (2017). DDoS in the IoT: Mirai and Other Botnets. Computer, 50(7), . Retrieved 25 March, 2020, from https://ieeexplore.ieee.org/abstract/document/7971869.

Iwanicki, K. "A Distributed Systems Perspective on Industrial IoT," 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, 2018, pp. 1164-1170.

Forrester, N. (2020). Malware targeting IoT devices skyrockets as transactions rise 1,500%. Retrieved 25 March, 2020, from https://securitybrief.com.au/story/malware-targeting-iot-devices-skyrockets-as-transactions-rise-1-500

Fruhlinger, J. (2018). The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet. Retrieved 25 March, 2020, from https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Nguyen, H., Ngo, Q. & Le, V. A novel graph-based approach for IoT botnet detection. *Int. J. Inf. Secur.* (2019). https://doi.org/10.1007/s10207-019-00475-6

Marinho, R. (2017). Exploring a P2P Transient Botnet — From Discovery to Enumeration. Retrieved 25 March, 2020, from https://morphuslabs.com/exploring-a-p2p-transient-botnet-from-discovery-to-enumeration-e72870354950

Shodan. (2020). Shodan search page. Retrieved 25 March, 2020, from https://www.shodan.io/search?query=esp8266

Spacehuhn. (c2020). Spacehuhn / esp8266_deauther. Retrieved 25 March, 2020, from https://github.com/spacehuhn/esp8266_deauther

Speers, T. (2019). How RISC-V Security Stacks Strengthen Computer Architecture. Retrieved 25 March, 2020, from https://www.allaboutcircuits.com/industry-articles/how-risc-vs-security-development-of-processor-computer-architecture/