National College of Ireland

Project Submission Sheet

Student Name:	Matthew Browne		
Student ID:	x21174415@student.ncirl.ie		
Programme:	MSc/PGD in Cybersecurity	**Year:**	1
Module:	Malware Analysis (H9MWAN)		
Lecturer:	Michael Pantridge MSc/PGD		
Submission Due Date:	08th August 2025		
Project Title:	Carry out an investigation into a botnet, Mirai		
Word Count:	5705		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: Matthew Browne

Date: 8th August 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. You must ensure that you retain a HARD COPY of ALL projects, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. Late submissions will incur penalties.
5. All projects must be submitted and passed in order to successfully complete the year. Any project/assignment not submitted will be marked as a fail.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

[Malware Analysis (H9MWAN)]

Your Name/Student Number	Course	Date
Name: Matthew Browne Student Number: x21174415	MSc/PGD in Cybersecurity	08/08/2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

I. AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool

II. Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

III. Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

IV. Additional Evidence:

[Place evidence here]

Continuous Assessment Name	Carry out an investigation into a botnet: Mirai
Student Name	Matthew Browne
Student ID	x21174415
Student Email	x21174415@student.ncirl.ie

Carry out an investigation into a botnet, Mirai

Matthew Browne
Microsoft MVP & CITP
x21174415@student.ncirl.ie

Abstract

Based on the requirements of our continues assessment we were required to Carry out an investigation into an assigned botnet which in my case was the Mirai Botnet for my use case I used a combination of google scholar , searches across the internet and articles related to Mirai Botnet , this allowed me to gather information in relation to its target device types , the type of malware it covers , the devastation its already caused around the world and how its evolved over time and what safeguard measures can be put in place to stop this malware in an enterprise setting.

1 Executive Summary

The objectives of the investigation was to understand how you would go about researching into a malware such as the Mirai Botnet , it was evident from the beginning that this was going to be a form of malware but what type of devices or surface areas would this effect , how large was the attack surface , what quantifiable area of the attack surface could be assessed and become destructive should a malware of this form be unleashed against an enterprise or home environment , what was the a monetary value towards the disruption of the attack all of these points were assessed again a litany of investigative methods and botnet investigative efforts were included alongside what coherent conclusion could I come to after researching about the botnet and how to minimise its destructive nature against potential recovery point objectives within environments and or backup methodologies and safeguards against these bots.

My key findings in summary resulted in me being able to understand that Mirai Botnet does have an element of resiliency with its ability to be able to obfuscate its names for the malware, I also discovered thanks to the DynDns that it could have resulted in upwards of 1.2 million per second of cost to the organisation. Part of some the observations were that if effected heavy hitters like amazon and Netflix, show casing it had no issues with going after bigger companies , the research highlighted a need for professionals and organisations to implement security hygiene as standard which included doing away with and form of default unsecure credentials , implementation of security posture management and eagle eye view of your IOT and endpoint states.

It also highlighted the implications which were observed for the Mirai Botnet such as research performed on 3 academic papers, consolidation of that research, identifying when papers were referencing or using contradictory research which required additional vetting. The research did showcase to me some website which couldn't be relied upon, and it did also highlight how you would go back to the basics of the CIA Triad and McCumber cube in terms of assessing the security posture of your IOT and endpoint devices.

2 Methodology

2.1 Strategy to search

So, for my strategy I based some of my research on a paper called "An In-Depth Analysis of the Mirai Botnet " [1]for me this was an interesting paper, in the abstract the researchers spoke about how IOT security is not spoken about in the world of information security this was back when IOT in 2017 wasn't really something enterprise nor individuals in home settings spoke about securing , I placed this article as my top contributor for research into the understanding of the Mirai Botnet malware , I supplemented this with other research into understanding the flow of the malware such as "Understanding the Mirai Botnet" [2] and how you would conclusively protect yourself against this malware. Interlinking both the CIA Triad (Confidentiality Integrity and Availability and the McCumber Cube [3] were two great ways of understanding and bringing together scenarios on how the Mirai Botnet could be prevented , this also formed part of my research into the prevention strategy for researching the malware. I did also discover as part of the process that Mirai has a "Don't Mess" list this essentially is a list of all Ip addresses and networks which it will not scan or look for e.g. US Department of Défense [4]

2.2 Datasets Analysis

For my continues assessment the Data analysis I did was more on the around the Mirai Botnet handler processes as you had one which was a bot handler , one which was an Admin handler and the other which was an Api handler all of which had unique requirements roles and responsibilities , it was the analysis of understanding how these were in conjunction with each other and what handler plays what role.

3 Botnet Investigation

3.1 Bots Identification

To be able to understand the Mirai malware botnet you first have to understand its capabilities and how it can move around latterly to devices, you also had to understand the level of impact it could have when it spread across systems. By form of research I was able to identify that this paper looked at an instance where on September 20th in 2016 a journalist named "Brian Krebs" [5] his website was hit with a DDos attack to get factual evidence on this I did look this up as I found a small anomaly with the date in the research paper, I was able to identify that it was actually hit on the 20th which was correct but it was reported and or written about on the 21st a single day later. It's understood as written by Brian and other researchers that the original code for this malware was released publicly by "Anna-Senpai" [6] with the source code being released Brian was able to uncover the identities of those who at least contributed to the creation of this botnet.

The type of file format the Mirai botnet usually identifies as is "The ELF file format", it usually has a name of "text or httpd" this to me suggests it primarily targets Linux based systems, this allows it also to blend in often with other file types and associations without raising suspicion. In the research paper for "Understanding the Mirai Botnet" this goes into more detail about it. some of the characteristics of its anti-virus evasion are the ability for the malware to be able to be able to blend in by utilising file name types which do not stand out or which can be given generic names, these vary and can include names such as "text , update or maybe even netstat" allowing it to evade traditional antivirus software. [7]

3.2 Botnet Size and Damage

Determining the size of the Mirai botnet or malware is a difficult task as this has been growing sense it first surfaced on the "8TH January 2016" [2] To understand what the attack is you have to understand what a "BotNet" a Botnet can be best described as a group of systems which are connected around the world but have been infected by malware , these systems then are controlled by a central server known as a "CNC" server which allow cybercriminals to be able to manipulate and control these systems. The cybercriminal then initiates the attack to a targeted domain, device or network which results in what's known as a "Distributed Denial of Service Attack" [8] , its known as this because the cybercriminal has instructed multiple bots to attack a source destination which essentially prevents legitimate traffic through to the destination server, this could be understood in the terms of an Amazon customer goes to use the amazon.co.uk domain but discovers there unable to reach the website due to a DDos attack , therefore preventing legitimate traffic from going through.

where this could be better understood is utilising the CIA Triad, confidentiality Integrity and Availability if we think in terms of a DDos attack utilising a Mirai botnet , the customer is unable to access the site because the botnet has instructed multiple IOT connected devices to attack the amazon domain, this is just one of many scenarios which can occur thanks to this malware , after the CIA Triad the McCumber Cube [3] which was built on the CIA Triad's foundations served as a model for information assurance programs which are utilised in protection against DDos attacks and methodologies just an example of how the Mirai botnet could be prevented. Based on the research paper I was able to understand that one of its largest attacks in history was on a Dynamic DNS providers website called "DyN Dns" [9] which caused significant damage to websites across the internet in terms of uptime some of the websites effected were "PayPal, Twitter , Amazon, Netflix" , this was known as the largest in history to date , its understood that no real value was ever placed on the cost of this attack but if effected over 50+ premium domains and services. [10] a best guess on this based on Cisco's analysis is on average it could cost about $250,000 to over $999,000 per hour but this can be differential and based on the profile of the target domains [11]. The attack itself resulted in a widespread outage od websites across multiple domains, users were affected which may have resulted in access to accounts such as PayPal, payment systems for making and receiving payments like banks, content delivery networks such as Netflix and shopping services such as Amazon effecting both public and private consumers and organisations.

3.3 Target Devices

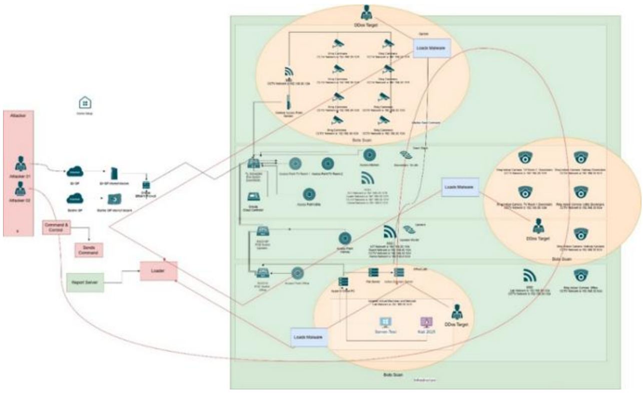
The type of devices that Mirai relies on are internet of things devices which have not had their default username and passwords changed or they were setup using very weak credentials e.g. Fridges like "Samsung Family Hub" , Freezers like "Samsung Hub", Security Cameras Like Ring / Swan / Hikvision, Like Ring or Eufy Video Doorbells, some of which are prime devices for launching this type of malware against , the Mirai malware looks to execute its malicious code against these devices once the code is up an running these devices then join part of the network of other infected devices. These all-form part of the "C&C server" which is then used to target sites and services across different locations on the internet. [12] , the cybercriminal instructs these devices to attack utilizing the DDos method. It is believed that in over 164 countries Mirai botnet has been found and this is increasing daily. [4]

3.4 Botnet Architecture

The Mirai botnet was primarily known for its ability to be able to perform DDoS attacks on websites across the internet the reason it became known for this was its ability to be able to make websites and other services unavailable it primarily focused on new devices which were introduced to the internet basically the ones with no changes to the default login credentials. The Mirai infrastructure was simple it had a server which is reported to , on that server there were two sockets one for listening and one for routing , the server listened for requests on port 23 which is a Tcp port and then routed them accordingly to the handler this then allowed the other socket to send the attack command on port 101 which is a CnC port establishing a listening / scanning exercise followed by a communicative attack and control exercise.

How the connections occurred was once on port 101 the attacker / server was able to communicate with the target device it would then save the session information which would be stored in a file on the server it would then follow through and execute the malware this would then have been a repetitive task for every machine it scanned.

3.4.1 Diagram of Mirai Botnet/Architecture Attack Sample



3.5 Botnet Behaviour

The Mirai botnet's behaviour was significantly highlighted in both "An In-Depth Analysis of the Mirai Botnet" and

"Understanding the Mirai Botnet" research papers the paper which discussed the In depth analysis provided some examples and behaviour into how the botnet could be disruptive, one example of this was 2 different universities on 2 different occasions were able remotely gain access into a medical "Pacemaker" this highlighted the need for security around internet connected devices to be discussed and addressed Rapid seven also highlighted this when they tested it out on an "Insulin Pump" [1] this showcased the dangerous and adverse effects the Mirai Botnet could have on and to human life in a real world scenario.

Mirai botnet's behaviour and its previous referencing by some academic researches can be called into questioning this is based on the "Malware Must Die" post which I read which made reference to incorrect flows and explanations of how the "watchdog timer works" [13] its clear to see that there are inaccurate information and papers written about this and caution should be taken to verify the integrity of the information. It should be said that Mirai botnet's abilities lie primarily within the networking space as this is where it does the most damage, while having smaller interaction with file systems for exploring, scanning and exploiting its clients.

3.6 Botnet Resilience

The Mirai botnet utilizes a command-and-control server to do its bidding, Mirai is compiled of two different elements the "Go element", this utilizes googles proprietary command line language which as previously stated works with both port 23 and port 101 which are TCP and Telnet ports. For the checks and requirements certain conditions need to be satisfied to distinguish between whether the servers are human operated or machine operated this allows the attacker (bot or handler) to depict and decide between the connections. From research I was able to figure out the Mirai botnet does not have a mechanism for reboots it simply restarts the scanning process all over again meaning that it would be reliant on other machines to be infected. In terms of C&C protection it does support some bulletproof hosting which prevents the malware from being taken down by internet service providers allowing for a longer uptime, it also sports some hardcoded binary files which allow it to have an additional layer of resilience against other malwares , it should be noted that Mirai didn't have allot of these and has evolved over time but it now makes up for some of this with its ability to expand rapidly.

3.6.1 What is a bot handler

This sends out a "4 Byte integer" this allows for the bot handler to understand if the process has been achieved and is completed once this is confirmed the bot handler waits to see if any additional bytes of data are sent normally this should be two with a time wait of 120-180 seconds outside of this the handler closes any stale connections and reports the client as not being alive , this allows the bot handler to track its active connections similar to what's used in uTorrent. [1]
What is an Admin handler

3.6.2 What is an Admin handler

An Admin handler works opposite to the way in which the bot handler works if anything above a "4 Byte integer" is presented to the socket the server is instructed to send out a new screen which allows the server to clear older screens and return to the working session , essentially allowing the server to create new users regardless of whether the new sessions work they can always revert back to older sessions. Because it uses a form of SQL allowing both Admins and none Admins the ability to be able to create accounts on the system.

The Bot handler vs Admin handler allows for a form of Bot resilience as the bot handler tracks for connectivity and the admin handler controllers the shell access to the server to be able to perform administrative actions.

3.6.3 What is an API Handler

The Application Handlers sole task is to initiate the attack utilizing plain text format this forms part of the process it should never exceed "3600" seconds. The Api handlers attack requires that it checks with a list of IP Addresses and then continues to perform an attack on the systems using predefined hardcoded login information, once the API Handler has been able to find additional IP Addresses on the range of the existing machine it completes the process once again growing and scanning machines on the subnets. [1]

3.6.4 Attack Flags (Form of Deception)

Some of the resilience factors in which The Mirai botnet deceives its targets is by having a predefined attack vector which include a dictionary of possible outcomes when attacking its IOT devices , should a device present specific tags it will set the value , if it does not it will set a null/default value , ensuring its prepared for as many scenarios as possible. Some of the attack flags supported are "UDP/VSE Flood, Dns Flood, Udp Plain and Gre" , The Mirai botnet does indeed support additional flood technologies such as Syn Tcp and Http.

Flag Type	Flag Result
UDP / VSE Flood	Both of these are identical with one difference. Udp allows the attacker or malicious actor to send random and unstructured data. Vse requires that the data is sent as a structured sting by the attacker or malicious actor.
DNS Flood	Acts similarly to the UDP Flood in terms of sending the data via port 53 same action here but it also requires that random data is loaded when sending blocks to DNS Servers.
UDP Plain	Creates packets fill these with random data entries / artifacts and send them over it then binds the socket with it as a default action or may even do this randomly. This allows it to ensure that the source port is not used when it wants to send over

	additional packets which may contain some data.
GRE	The operation of sending extremely large payloads in which the router needs to address, this normally results in a larger processing requirement, often this is seen in site to site or site to client vpn technologies.

3.7 Botnet Takedown

The Mirai botnet was indeed taken down back in 2016 by the FBI this was from a result of which they achieved in a courtroom in “Anchorage” this resulted in three students who had plotted the whole invasion which resulted in pleading guilty after an attempt on IOT devices such as camera’s and routers were breached which part in parcel caused issues for internet service providers in the Us and Europe to address due to the attacks performed by the Malware. It’s said that the nation state ties resulted in the easier location of the individuals due to the illicit conduct which made it easier for the FBI to catch them. [14] Previous to this Brian Krebs did make attempts to at least identify some of the co-conspirators involved in the attack [5] in terms of efforts to deactivate the botnet this only came into fruition in 2016 when the three students were taken to court , the Malware lives on but has diminished over time.

3.8 Botnet Evolution

Based on my research it was evident that there are various newer “Models” of the Mirai botnet , this is a combination of existing and modified version Mirai originally surfaced in 2016 with the Krebs attack in September of 2016 being one of its heavy impacts this was followed swiftly by the DDos attacks on Dyn DNS in October of 2016 It wasn’t until February of 2017 that the attackers were identified and sentenced for the actions they played. [2] Mirai infection rate was at an estimated all time high of 600,000 at its highest point back in 2016 this fellow to just 100,000 in February of 2017. [2]

4. Best Practices for organizations and individuals / Recommendations

Utilizing the research paper for “Motivating a Market or Regulatory Solution to IoT Insecurity with the Mirai Botnet Code” [15] I was able to identify that this spoke about ways in which an individual and or organization could inform its users of devices which had known CVES which were vulnerable that needed to be patched. This would provide for a useful way to know if any government agencies had interacted with the systems and a log file would be left on the system. Due to the nature of which this was found its was deemed that the government did not want to utilize this an accepted method because then they would have to inform device owners.

4.1 Changing default login credentials

Changing default login credentials is something that should be done from day one using the pre-defined username and password provided for devices from the manufacturer is never a good option as this is normally only provided to allow you to begin using the device. This will negate the ability for attackers and threat actors from being able to deploy malicious scripts, attack vulnerabilities within the oem software and prevent script kiddies from using dictionary-based attacks. The method to be able to do this is provided by manufacturers often through web-based setup on startup of their appliance or via directly connecting into the appliance on a specific port, this recommendation should be applied on receipt of any new device in the household or organization.

4.2 Utilizing a Firewall

Invest in a firewall for your network, should the need arise to be able to control the devices across your network such as segregation between Vlan’s or maybe access control lists for websites, or maybe even segmenting your SSID networks for wireless lan networks a firewall is often a future proof investment into securing your home or business network this allows you to secure your lan utilizing switches and ports prescribing Vlan’s where required , introducing Mac filtering/Binding or maybe even include some content filtering within the home it also allows you to segment and elevate your networks perhaps one for adults and one for kids.

4.3 Utilizing an EDR Solution

Monitor Utilizing an intrusion detection system, often this can be integrated into the firewall appliance. Utilizing and setting up a Honeypot can be an optimal way of ensuring attackers do not gain access to your local Lan or Wan network, implementing alongside this a DMZ may ensure only required devices have internet access externally although I prefer that no devices have external access unless required and proper rules are configured across the Wan/Lan.

4.4 Utilizing Antivirus/Endpoint Detection and Response software vendors

Utilizing an Endpoint Detection and Response or Antivirus all in one solution gives you the ability and freedom to be able to secure your servers using baselines, locking down your workstations and cloud resources using Nist controls. Ensuring your AV or EDR solution includes your IOT devices to ensure they are all protected under the single cloud or software umbrella and or console this will ensure that your devices are not known to vulnerable CVES or known threat actors.

5. Conclusions & Findings

The Analysis and research I did into the Mirai Botnet afforded me the ability to see that threats do indeed exist for Internet of Things Devices, by going through academic research papers of which I used three I was able to determine some of the threats posed by the Mirai Botnet and how these can lead to costly implications for organisations. The Mirai botnet showcased to me the importance of removing default login credentials for everything it highlighted the need for user awareness because if this is not actioned by users it leaves them open in both an organisation and home setting to vulnerabilities.

The Mirai Botnet architecture is designed with resilience in mind despite its copy and paste code which was leaked openly on the internet , in saying this it showcases how it was able to use simple command and control structures to be able to control is clients the layering around both the bot and admin handler showcase how it is designed to handle multi complex scenarios and how its binaries are equipped with the ability to differentiate themselves between these utilising dictionary attacks for simple lookup.

The DDos attacks which happened to DynDNS demonstrated the ability for the Mirai Botnet to be able to disrupt at scale large organisations and domain such as Amazon PayPal and Netflix, all of which had real world consequences, Mirai's ability to be able to hide in plain site and evade traditional antivirus and Edr platforms also demonstrated its capability in evasion techniques.

Implementation for both organisations and individuals of basic security hygiene like default credential changes, advanced firewall and intrusion systems alongside network segmentation will all allow for a robust defence against potentially known bad actors and malware like Mirai.

Regardless of the findings I did find Some limitations and implications which should be addressed.

My ability to not be able to currently analyse Mirai Botnet in a real or lab-based environment presented for a blocker for some of my investigation, getting under the hood and understanding each of the sequences would have been beneficial. My research relied on 3 academic papers of which while all interesting some of the points contradicted others the methodologies across 2 of the papers looked at the Mirai Botnet in different fashions and this did result in some doubling up on reading and work.

Experience around understanding Pcap files would have been beneficial this is something I've self-identified as an area I should investigate understanding more and trying to get lab instances going to be able to know how to analyse these in the future. It was evident from the research that some entities like "MalwareMustDie" had their own agenda, and the information was not always accurate, this was also highlighted in the research papers that I had picked, and some cross research and referencing would need to be done if you were doing additional investigations into understanding the procedures and analysis.

For cybersecurity professionals the implications were simple, adhere to good device hygiene by removing pesky default logins and ensuring firmware's are up to date on devices. For organisations IOT devices should be looked and accessed the same as server or workstation endpoints, having adequate security controls and filtering in place is crucial, ensuring devices which run on legacy equipment should be placed into the correct Lan / Dmz where necessary for security posture management.

For vendors like Cisco, SonicWALL, Dell, Hp and others they should all ensure that password changes are mandatory for their equipment and that simple passwords are disallowed, there should also be greater visibility into how these devices are managed and secured from the outset e.g. vendor management portals and firmware updates should ship by default with devices.

What would I do if I had more time

I would have liked to test out and try performing some static and dynamic analysis on the malware itself but that would have been contingent on having an isolated environment specially that I could afford to re-build.

More training around understanding the CNC communication with servers which had the Mirai Botnet installed and using Wireshark Pcap to be able to analyse them and see how the communication was occurring. Speaking with subject matter experts or other researchers would have been a beneficial option to be able to understand from there findings how they configured tested and setup their environments for this analysis. All these points should I have had more time would have provided for a more rounded understanding of the Malware. For me this investigation was more of a basic and foundational introduction into the world of Mirai Botnet's. References

References

[1] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim and J. N. Kim, "An In-Depth Analysis of the Mirai Botnet," 24-25 July 2017. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8392610. [Accessed 7th July 2025].

[2] Usenix, "usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf," Usenix, 16-18th August 2017. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf. [Accessed 7th July 2025].

[3] en.wikipedia.org, "en.wikipedia.org/wiki/McCumber_cube," en.wikipedia.org, 01 May 2024. [Online]. Available: https://en.wikipedia.org/wiki/McCumber_cube. [Accessed 7th July 2025].

[4] imperva.com, "imperva.com/blog/malware-analysis-mirai-ddos-botnet/," imperva.com, 26th October 2016. [Online]. Available: https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/. [Accessed 7th July 2025].

[5] B. Krebs, "KrebsOnSecurity Hit With Record DDoS," 21 September 2016. [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. [Accessed 7th July 2025].

[6] B. Krebs, "Source Code for IoT Botnet 'Mirai' Released," 1st October 2016. [Online]. Available: https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/. [Accessed 7th July 2025].

[7] D. Maciejak and J. Salvio, "https://www.fortinet.com/blog/threat-research/the-ghosts-of-mirai," 24th June 2021. [Online]. Available: https://www.fortinet.com/blog/threat-research/the-ghosts-of-mirai. [Accessed 7th July 2025].

[8] wikipedia.org, "en.wikipedia.org/wiki/Denial-of-service_attack," wikipedia.org, 06 06 2024. [Online]. Available: https://en.wikipedia.org/wiki/Denial-of-service_attack. [Accessed 7th July 2025].

[9] en.wikipedia.org, "DDoS attacks on Dyn," en.wikipedia.org, 22 October 2016. [Online].

Available: https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn. [Accessed 7th July 2025].

[10] "en.wikipedia.org/wiki/DDoS_attacks_on_Dyn," wikipedia, 21 October 2016. [Online]. Available: https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn. [Accessed 7th july 2025].

[11] A10, "a10networks.com/blog/5-most-famous-ddos-attacks/," A10, 21 January 2022. [Online]. Available: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/. [Accessed 7th July 2025].

[12] Radware, "radware.com/security/ddos-knowledge-center/ddospedia/mirai/," Radware , 7th July 2024. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/mirai/. [Accessed 7th July 2025].

[13] malwaremustdie.org, "blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html," blog.malwaremustdie.org, 1st September 2016. [Online]. Available: https://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html. [Accessed 7th July 2025].

[14] Alaska World Affairs Council , "Combating International Cyber Crimes – Taking Down Mirai Botnet | FBI Supervisory Special Agent William Walton," Alaska World Affairs Council , 19th October 2018. [Online]. Available: https://alaskaworldaffairs.org/archived-events/fbi-cyber-crime/. [Accessed 8th july 2025].

[15] J. A. Jerkins, "ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7868464," ieeexplore.ieee.org, 11 January 2017. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7868464. [Accessed 8th July 2025].

4 Works Cited

[1] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim and J. N. Kim, "An In-Depth Analysis of the Mirai Botnet," 24-25 July 2017. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8392610. [Accessed 7th July 2025].

[2] Usenix, "usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf," Usenix, 16-18th August 2017. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf. [Accessed 7th July 2025].

[3] en.wikipedia.org, "en.wikipedia.org/wiki/McCumber_cube," en.wikipedia.org, 01 May 2024. [Online]. Available: https://en.wikipedia.org/wiki/McCumber_cube. [Accessed 7th July 2025].

[4] imperva.com, "imperva.com/blog/malware-analysis-mirai-ddos-botnet/," imperva.com, 26th October 2016. [Online]. Available: https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/. [Accessed 7th July 2025].

[5] B. Krebs, "KrebsOnSecurity Hit With Record DDoS," 21 September 2016. [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. [Accessed 7th July 2025].

[6] B. Krebs, "Source Code for IoT Botnet 'Mirai' Released," 1st October 2016. [Online]. Available: https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/. [Accessed 7th July 2025].

[7] D. Maciejak and J. Salvio, "https://www.fortinet.com/blog/threat-research/the-ghosts-of-mirai," 24th June 2021. [Online]. Available: https://www.fortinet.com/blog/threat-research/the-ghosts-of-mirai. [Accessed 7th July 2025].

[8] wikipedia.org, "en.wikipedia.org/wiki/Denial-of-service_attack," wikipedia.org, 06 06 2024. [Online]. Available: https://en.wikipedia.org/wiki/Denial-of-service_attack. [Accessed 7th July 2025].

[9] en.wikipedia.org, "DDoS attacks on Dyn," en.wikipedia.org, 22 October 2016. [Online]. Available: https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn. [Accessed 7th July 2025].

[10] "en.wikipedia.org/wiki/DDoS_attacks_on_Dyn," wikipedia, 21 October 2016. [Online]. Available: https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn. [Accessed 7th july 2025].

[11] A10, "a10networks.com/blog/5-most-famous-ddos-attacks/," A10, 21 January 2022. [Online]. Available: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/. [Accessed 7th July 2025].

[12] Radware, "radware.com/security/ddos-knowledge-center/ddospedia/mirai/," Radware , 7th July 2024. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/mirai/. [Accessed 7th July 2025].

[13] malwaremustdie.org, "blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html," blog.malwaremustdie.org, 1st September 2016. [Online]. Available: https://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html. [Accessed 7th July 2025].

[14] Alaska World Affairs Council , "Combating International Cyber Crimes – Taking Down Mirai Botnet | FBI Supervisory Special Agent William Walton," Alaska World Affairs Council , 19th October 2018. [Online]. Available: https://alaskaworldaffairs.org/archived-events/fbi-cyber-crime/. [Accessed 8th july 2025].

[15] J. A. Jerkins, "ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7868464," ieeexplore.ieee.org, 11 January 2017. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7868464. [Accessed 8th July 2025].