Article

Not peer-reviewed version

Understanding and Classifying Permanent Denial of Service Attacks

Stanislav Abaimov *

Posted Date: 9 February 2024

doi: 10.20944/preprints202402.0561.v1

Keywords: Cyber attack; Denial of Service; Exploit

Article

Understanding and Classifying Permanent Denial of Service Attacks

Stanislav Abaimov

University of Bristol; stanislav.abaimov@bristol.ac.uk

Abstract: In the evolving landscape of cybersecurity threats, the Permanent Denial of Service (PDoS) attacks have emerged as a particularly damaging form of cyber aggression. Unlike the more well-known Denial of Service (DoS) attacks, which disrupt services temporarily, PDoS attacks aim to inflict irreversible damage to systems, often resulting in significant system overhauls and requiring hardware replacement. To enable the development of effective security measures, but also to address the knowledge gaps, this paper offers an in-depth exploration of PDoS attacks, emphasizing their distinguishing characteristics, underlying mechanisms, and potential further development. Through a comprehensive case study, the research highlights diverse tactics and strategies employed by attackers, from targeting IoT devices to manipulating boot processes and exploiting firmware vulnerabilities. A novel classification of PDoS attack vectors is proposed, that also explains the ways in which the systems can be compromised. The findings confirm the pressing need for adaptive and robust defense mechanisms to mitigate the threats posed by PDoS attacks in our interconnected digital world.

Keywords: cyber attack; denial of service; exploit

1. Introduction

In today's dynamic cyber threat environment, the Permanent Denial of Service (PDoS) attacks are recognized as particularly devastating cyber threats. Unlike temporary Denial of Service (DoS) attacks, which cause transient disruptions, PDoS attacks lead to irreversible hardware damage, significant economic repercussions, and in the contexts like healthcare and critical infrastructure, can even pose threats to human life. As adversarial methods continue to advance, it becomes essential for the detection and defense mechanisms to evolve.

Despite the severe implications of such attacks, exemplified by the incidents like the 2017 NotPetya malware outbreak which resulted in billions of USD in global damages by irreparably compromising thousands of computers [1], a dedicated research on PDoS remains significantly less compared to its temporary counterparts [2]. This lack of systematic study leaves a deep gap in the scientific knowledge and the industries, governments, and individuals vulnerable to this specific threat.

Recognizing this knowledge gap and the risks associated with the PDoS attacks, this paper endeavors to provide a comprehensive study of the anatomy of the PDoS threats. Our multidimensional framework, designed specifically for the PDoS attacks, seeks to equip both academic researchers and industry practitioners with the expertise required to predict, identify, and defend against these high-impact threats.

Our primary contributions are:

1. A detailed exploration of PDoS attack vectors, evaluated with real-world case studies, encompassing tactics like Internet of Things (IoT) exploitation [3,4], boot process disruption [5], and strategic data destruction [6].
2. Introduction of a novel classification framework for PDoS attacks, categorizing threats across dimensions such as access channel, impact scale and significance, and target devices.
3. A thorough analysis of the challenges in detecting the PDoS attacks, emphasizing the complexity of evasion tactics [7], varied attack vectors, similarities with legitimate processes, and the constant evolution of associated malware [8].

Our research provides a thorough academic understanding of the PDoS attacks, while also suggesting future research to enable the development of specialized detection methodologies, informed mitigation plans, and impactful metrics to quantify PDoS repercussions. With increasing instances of PDoS attacks [9], this in-depth analysis is timely and essential for the global cybersecurity community.

2. Background

Permanent Denial of Service (PDoS) attacks, characterized by their potential to cause long-term or irreversible damage to systems, represent a critical cybersecurity challenge. Distinct from temporary denial of service (DoS) attacks, employing a wide array of sophisticated strategies, the PDoS attacks target both software and hardware. These strategies extend beyond mere disruption, aiming for permanent impairment.

Modern PDoS adversaries often employ subtle, long-term tactics to bypass traditional intrusion detection systems, including IP spoofing and mimicking legitimate traffic. They range from distributing malware that corrupts firmware, boot processes, or data to direct hardware manipulations, such as voltage/current alterations. More advanced evasion methods, as seen with malware like Gapz [7], compromise the OS at the kernel level, making detection even more challenging.

This section provides an overview of the historical context and contemporary challenges posed by the PDoS attacks.

2.1. Historical Context

The intersection of software vulnerabilities and hardware threats has always been a significant concern in the realm of cybersecurity. The first reports of these being successful appeared in public sources about three decades ago but remain rare due to various reasons discussed later. The known noteworthy occasions where software-induced actions have resulted in tangible hardware damage include:

- CIH/Chernobyl Virus (1998) [10]: A prominent example of a destructive malware, this virus targeted the Windows 98 systems. While primarily causing data corruption, in some cases, it could overwrite the BIOS, rendering the system inoperable.
- Commodore PET's "Killer Poke" (Late 1970s): In the early days of personal computing, certain memory interaction commands on the Commodore PET, particularly PEEK and POKE, were rumored to damage the system's hardware.
- GPU Stress-Test Applications: Tools, such as FurMark, underscored the potential of software to exert physical stress on hardware, particularly GPUs. When misused, they can lead to overheating.
- Overclocking and Voltage Manipulation: Theoretical malware could force CPUs or GPUs to operate beyond safe thresholds. Though the modern systems typically have mechanisms to counter such threats.
- Hoaxes and Mythical Threats: Many purported threats, like the "Data Crime Virus" of the 1980s, turned out to be baseless, despite causing initial alarm.

Recognizing that the threats to hardware from the software actions exist, protective measures have been incorporated into the modern hardware often to mitigate these risks and prevent such damage.

2.2. Contemporary PDoS Challenges

The increasing democratization of cybercrime tools means that even less-skilled adversaries can launch potent PDoS attacks. E.g., off-the-shelf DDoS tools and DoS malware are now easily accessible on the dark web, lowering the entry barrier for potential attackers.

High-profile incidents, such as the 2017 NotPetya [11] outbreak and the 2015 BlackEnergy attack on the Ukrainian utilities [12,13], highlight the evolving and dangerous nature of the PDoS attacks.

Cyber-physical systems, industrial networks, and Internet-of-Things devices become increasingly vulnerable, presenting a significant risk of failure and societal impact. Both the legacy systems and modern IoT devices are vulnerable, exacerbating the complexity of defense strategies. Addressing these challenges requires a multi-layered approach encompassing software, hardware, network, and human factors to create a robust and resilient cybersecurity posture.

2.3. Related Work

While the academic publications addressing PDoS (Permanent Denial of Service) attacks directly are limited, this survey was carried out to address this gap. This survey includes the academic articles, whitepapers, and technical reports available in the open public sources. The most widely used exacmple is the malware BrickerBot [14], which has undergone considerable investigation, most notably in the study by Sachidananda et al. [15]. This research offers an in-depth analysis of BrickerBot's capabilities, targeting methods, and potential impact. However, this research, as well as most of the analysed studies, have a focus on a specific area and often lack a comprehensive holistic study.

Due to the limited number of malware cases that cause direct physical damage to devices, the scope of the literature review was expended to include the cyber attacks that prevent devices from booting the operating systems and similar cases [5,7].

Another gap in the current academic literature is the lack of consistent methodology for studying the PDoS attacks. The individual studies are often constrained by their own scope, which may be limited to specific types or categories of attacks, and only mention the possibility of PDoS [16].

Despite these limitations, the existing literature creates a path to understanding the mechanics of PDoS attacks, such as the methods used for propagating the malware or the intricacies of the attack vectors. However, they often do not present a unified framework for classification or analysis, making it challenging to compare different PDoS threats directly.

To build a reliable defense system, these attacks should be thoroughly studied and classified. This necessitates the development of an overarching framework that encapsulates the various characteristics of PDoS attacks as they are understood today, including the tactics that adversaries employ to cause the lasting system damage. Consequently, our study aims to fill these gaps by providing a more holistic understanding and classification of PDoS threats.

3. Overview of the Framework

3.1. Attack Vectors

To safeguard against the insidious nature of Permanent Denial of Service (PDoS) attacks, an understanding of the myriad of attack vectors is essential. This section delves into these vectors, highlighting tactics adversaries employ to deliver lasting system damage.

A multitude of attack vectors, targeting a wide range of devices, highlights the need for versatile detection mechanisms. Physical attacks, like the USB Killer, and subtle software manipulations often evade traditional detection frameworks, underscoring the need for a multi-pronged detection approach.

PDoS attacks, with their multifaceted nature, necessitate a granular classification for effective defense. This section seeks to provide a comprehensive framework that categorizes these attacks based on their unique characteristics and employed vectors.

PDoS threats can incapacitate devices through various means, including direct physical access, command execution, or system file manipulation. We broadly classify these methods into Direct Controlled Access and Indirect System Setting Modification.

3.2. Detection Challenges of PDoS Attacks

Detecting PDoS attacks is inherently complex due to their intent to deliver lasting, and often irreversible, damage. This section dissects the multifaceted challenges posed by PDoS assaults, drawing insights from recent high-impact malware case studies.

Modern PDoS adversaries often employ subtle, long-term tactics to bypass traditional intrusion detection systems, including IP spoofing and mimicking legitimate traffic. More advanced evasion methods, as seen with malware like Gapz [7], compromise the OS at the kernel level, making detection even more challenging.

PDoS attacks often exploit legitimate system processes or commands, making them difficult to detect without broader context. Distinguishing between genuine and malicious operations, especially in scenarios like firmware updates, presents significant detection challenges.

3.3. Rapid Evolution of Malware

The continuous evolution of PDoS malware, as demonstrated by our case studies, emphasizes the need for adaptive detection mechanisms. As defense strategies evolve, so do the tactics of attackers, necessitating a proactive and ever-evolving approach to detection.

Detecting PDoS attacks, given their lasting impact and diverse tactics, is a pressing challenge. The dynamic nature of these threats demands equally dynamic and evolving detection and mitigation strategies. Our case studies illuminate the evolving nature of PDoS attacks, underscoring the need for continuous innovation in defense mechanisms.

4. Design of the Framework

PdoS attacks, with their multifaceted nature, necessitate a granular classification for development of effective defense. This section seeks to provide a comprehensive framework that categorizes these attacks based on their unique characteristics and employed attack vectors. This detailed categorization assists researchers and practitioners in understanding the nature, patterns, execution, and potential impact of these attacks.

The first classification criteria considers the PDoS capacity to disable devices through various means, including direct physical access, command execution, or system file manipulation. We broadly group these methods into Direct Controlled Access and Indirect System Setting Modification.

The following criteria were used for the for the proposed classification: the type of attack vector, method of propagation, payload delivery mechanism, and targeted systems among others, as defined below.

4.1. Attack Vector

The attack vector describes the pathway or method used by the attacker to access or harm the target. Detailed in the “Attack Vector Taxonomy” section, this category breaks down the diverse routes attackers employ to launch the PDoS attacks. Understanding the specific vector of an attack is vital. Different vectors may require varied detection methods, and by classifying attacks based on their vector, we can tailor defenses more effectively.

4.2. Type of Attack

This category focuses on the specific methodology or technique used in the PDoS attack. Whether it’s Boot Process manipulation, IoT exploitation, Disk wiping, etc., understanding the type helps in identifying the specific nature of the attack. Recognizing the type of attack helps in narrowing down potential mitigation strategies and understanding the attacker’s intent and expertise.

4.3. Complexity

This category measures the sophistication of the attack. Attacks can be classified as simple, moderate, or complex based on their execution, required expertise, and the intricacy of the employed technique. Understanding an attack's complexity can provide insights into the attacker's skill level and resources. More complex attacks might indicate well-funded and organized threat actors.

4.4. Propagation

Propagation refers to how the attack or malware spreads. This could be manual (requiring human intervention), self-propagating, or a combination of both. The propagation method can give insights into the attack's potential reach and speed of spread, essential for containment and mitigation strategies.

4.5. Payload

This category examines the specific malicious activity or load the attack delivers. It could involve direct interaction, acting as a dropper, or downloading additional malicious components. The payload reveals the immediate objective of the attack, whether it's to deliver another malware, exploit a vulnerability, or directly harm the system.

4.6. Target

This classification focuses on the specific aim or target of the attack. It could be hardware components, firmware, industrial control systems (ICS), IoT devices, etc. Identifying the target helps in understanding the attacker's intent, whether it's to disrupt a specific process, damage hardware, or exploit a particular device type.

4.7. PDoS Class

PDoS attacks can be classified further into Direct PDoS and Extended PDoS based on their nature and lasting effects. This distinction helps in understanding the longevity and potential repercussions of the attack, allowing for tailored response strategies.

4.8. Impact

The impact of an attack reveals its consequences. It can range from device bricking, data inaccessibility, system compromise, to operational disruption, among others. Measuring the impact is pivotal in understanding the severity of the attack, guiding both immediate response actions and long-term mitigation strategies.

Based on the identified major characteristics of the attacks, it is possible to develop an evaluation template that can serve as a robust tool for stakeholders to assess, mitigate, and adapt to the evolving nature of PDoS threats. This framework not only helps in immediate threat assessment but also guides researchers and developers to future-proof defensive technologies.

4.9. Malware Evaluation Template

To systematically and uniformly assess the threat landscape of the PDoS malware, a standardized template can be used to captures the essence of each malware variant. This consistency not only facilitates a more in-depth analysis but also aids in drawing parallels or distinctions between various malware samples. The proposed template encapsulates the vital parameters of malware, ensuring a comprehensive evaluation. Each attribute in thise template provides an insight into the malware's nature, its potential impact, and the nuances of its design and deployment.

- **Year of Discovery**: [Year or Time Frame]
- **Attack Vector**: [Specific Method or Technique Used]

- **Type of Attack**: [Nature or Class of Malware, e.g., Ransomware, Worm, etc.]
- **Complexity**: [S (Simple) / M (Moderate) / C (Complex)]
- **Propagation Technique**: [Self / Manual / Combo]
- **Payload Delivery Mechanism**: [Direct Download / Dropper / Direct Interaction / Other]
- **Targeted System**: [Specific System or Device Targeted, e.g., IoT, ICS, Firmware]
- **Category**: [Direct PDoS / Extended PDoS / Other]
- **Impact**: [Specific Consequences or Ramifications of the Attack]

Justification

The malware evaluation template provides a structured approach to assess and classify different malware strains effectively. By breaking down the various characteristics of malware, it allows for a more comprehensive understanding of its functionalities and objectives. This systematic evaluation aids in the comparative study of different malware, highlighting their similarities and differences. Furthermore, by understanding each aspect of the malware, researchers and defenders can devise better detection, mitigation, and response strategies. This template acts as a crucial tool in the hands of cybersecurity professionals, ensuring a consistent methodology in malware assessment across the board.

To illustrate the applicability of the proposed methodology, we apply it to selected case studies.

5. Case Studies of PDoS Attacks

Permanent Denial of Service (PDoS) attacks have emerged as a significant threat in the cyber landscape due to their unique and lasting impacts on systems. Such attacks either cause immediate and irreversible damage or induce conditions that lead to system malfunctions. This section presents the case studies on the notorious PDoS malware to offer insights into their methodologies and impacts. A summarized overview of these case studies is provided in Table 1.

5.1. Chernobyl (CIH Virus): The Hardware Hijacker

The CIH, also known as the Chernobyl Virus, emerged in 1998, pioneering hardware-targeted attacks.

Attack Vector: CIH had the capability to overwrite system drive data and even attempt to flash the BIOS, rendering machines non-functional.

Target Systems: Primarily targeted PCs with the intent of direct hardware damage.

Impact: The CIH virus posed threats of significant hardware damage, making affected machines irreparable.

Relevance and Lessons: The advent of CIH highlighted the potential for malware to directly target and damage hardware components, a shift from traditional software-based attacks.

5.2. BrickerBot: An IoT Saboteur

BrickerBot, discovered in 2017, signaled a new wave of threats against the ever-expanding Internet of Things (IoT) ecosystem. Gaining notoriety for its ability to "brick" or render IoT devices non-operational, BrickerBot shed light on the pressing security challenges of IoT.

Attack Vector: This malware exploited devices with exposed telnet ports and default credentials. Distinctly, its sole intent was destruction, contrasting with other malware that typically harness IoT devices for botnets.

Target Systems: BrickerBot was specifically designed to compromise Linux-based IoT devices.

Complexity and Techniques: Its complexity stemmed from a multi-pronged attack strategy, including brute force attacks and storage corruption. Its aggressive propagation mechanism further augmented its threat potential.

Impact: The malware's ability to render devices unusable presented both economic and functional challenges, especially for businesses heavily reliant on IoT.

Relevance and Lessons: BrickerBot's existence underscored the urgency of bolstering IoT security. It emphasized the importance of changing default credentials, securing device ports, and regular updates.

5.3. Silex: The Linux System Wiper

Emerging in 2019, Silex posed a significant threat to Linux systems and IoT devices with its multi-vector destructive capabilities.

Attack Vector: After gaining root access, Silex corrupted system storage, wiped files, deleted firewall rules, and halted systems, rendering them non-functional.

Target Systems: Silex targeted both Linux systems and IoT devices, indicating an evolution in PDoS attack vectors.

Impact: The malware led to system-wide disruptions, often necessitating complete hardware replacements or reinstalls.

Relevance and Lessons: Silex's emergence showcased the evolving nature of PDoS attacks and the need for robust system security, especially in the Linux and IoT realms.

5.4. Mamba: The Disk Encryptor

Mamba, a unique ransomware variant, emerged with a distinct strategy of whole disk encryption.

Attack Vector: Instead of encrypting individual files, Mamba encrypted entire hard drives, rendering systems inoperable.

Target Systems: The malware was indiscriminate, targeting a range of systems, with the primary aim of data denial.

Impact: Mamba's attacks led to data inaccessibility, causing significant disruptions to affected entities.

Relevance and Lessons: Mamba's approach redefined ransomware strategies, emphasizing the need for robust data backup and recovery solutions.

5.5. Summary table

The summary presented in Table 1 provides a comprehensive classification of various Permanent Denial of Service (PDoS) malware, spanning several years and diverse attack vectors. This taxonomy encapsulates malware from the early stages, like the Commodore PET's "Killer Poke" from the 1970s, to more recent threats like Silex from 2019. The malware is characterized based on multiple facets such as their attack vector, target type, complexity, propagation method, payload delivery mechanism, target systems, category of the attack, and the resultant impact. The table underscores a notable shift in the PDoS threats over the years. Initially, the attacks were more hardware-oriented, like the CIH/Chernobyl Virus that caused direct hardware damage. However, as the digital landscape evolved, the PDoS attacks expanded their horizons, targeting boot processes, IoT devices, and even multifaceted systems. More recent attacks, such as BrickerBot and Silex, have leveraged IoT vulnerabilities, reflecting the growing integration of IoT devices in modern infrastructure. The table serves as a summary of the evolving and escalating nature of PDoS threats in the cyber realm.

Attack vector: To be filled based on the specific pathways used by malware to infiltrate the target system.

Target type: Indicates the intended victims of the malware, whether they are individual users, enterprise networks, or specialized systems like IoT or ICS.

Complexity of the Attack: This would involve designating attacks as either Simple (S), Moderate (M), or Complex (C) based on the number of techniques or vulnerabilities they exploit.

Propagation Techniques: Denote whether the malware self-propagates (Self), requires manual intervention (Manual), or employs a combination of both (Combo).

Payload Delivery Mechanism: This could indicate Direct Download (DD), Dropper (DR), Direct Interaction (DI).

doi:10.20944/preprints202402.0561.v1

Targeted System: This category will specify which system the malware targets, such as IoT, ICS (Industrial Control Systems), Firmware, or a combination thereof.

Category of the attack: direct, extended.

Resultant impact: Specifies the concrete outcomes of the malware attack, ranging from data corruption, system inoperability to more severe consequences like infrastructure shutdown.

Table 1. Expanded Classification of PDoS Malware Aligned with Attack Vectors, Complexity, Propagation Techniques, Payload Delivery, Target Systems, and Impact.

Malware	Year	Vector	Type	Complexity	Propagation	Payload	Target	Category	Impact
Commodore PET's "Killer Poke"	1970s	Memory Interaction Command	Hardware	Simple	Manual	DI	Hardware (Monitor)	Direct PDoS	Potential Monitor Damage
CIH/Chernobyl Virus [10]	1998	Hardware Manipulation	Hardware	Simple	Manual	DD	Hardware	Direct PDoS	Hardware Damage
TDL4 (TDSS/ Alureon) [7]	2007	Boot Process	Boot	Complex	Self	DD	Firmware	Extended PDoS	Stealth Operation
BlackEnergy [12,13]	2007	System Compromise	Multifaceted	Complex	Combo	DR	ICS	Extended PDoS	Operational Disruption
Stuxnet [17]	2010	System Compromise	Multifaceted	Complex	Combo	DR	ICS	Extended PDoS	Operational Disruption
Olmasco [7]	2011	Boot Process	Boot	Moderate	Manual	DR	Firmware	Extended PDoS	Stealth Operation
Gapz [7]	2012	Boot Process	Boot	Complex	Self	DD	Firmware	Extended PDoS	System Compromise
DarkSeoul [18]	2012	File	Data Destruction	Complex	Self	DD	Firmware/ICS	Direct PDoS	Data Inaccessibility
StoneDrill [1]	2012	File	Data Destruction	Moderate	Self	DD	Firmware/ICS	Direct PDoS	Device Bricking
Rovnix [7]	2014	Boot Process	Boot	Moderate	Manual	DR	Firmware	Extended PDoS	Stealth Operation
Mamba [9]	2016	File	Data Destruction	Moderate	Manual	DR	Firmware/ICS	Direct PDoS	Data Inaccessibility
Petya/ NotPetya [11]	2016	Boot Process	Boot	Complex	Combo	DR	Firmware	Extended PDoS	Data Inaccessibility
KillDisk [12,13]	2016	File	Data Destruction	Moderate	Self	DD	Firmware/ICS	Direct PDoS	Operational Disruption
Remaiten [4]	2016	IoT Exploitation	IoT/Linux	Complex	Self	DD	IoT	Direct PDoS	System Compromise
Amnesia [3]	2017	IoT Exploitation	IoT/Linux	Moderate	Self	DD	IoT	Direct PDoS	Data Inaccessibility
BrickerBot [14]	2017	IoT Exploitation	IoT/Linux	Complex	Self	DD	IoT	Direct PDoS	Device Bricking
Bad Rabbit [5]	2017	Boot Process	Boot	Moderate	Manual	DR	Firmware	Extended PDoS	Data Inaccessibility
USB Killer [19]	2017	Hardware Manipulation	Hardware	Simple	Manual	DD	Hardware	Direct PDoS	Hardware Damage
LoJax [20]	2018	Boot Process	Boot	Complex	Self	DD	Firmware	Extended PDoS	Stealth Operation
MBRLock	2018	Boot Process	Boot	Moderate	Manual	DD	Firmware	Direct PDoS	Data Inaccessibility
ZeroCleare	2019	Disk Wiping	Multifaceted	Complex	Self	DR	Firmware/ICS	Extended PDoS	Data Inaccessibility
Silex [21]	2019	IoT Exploitation	IoT/Linux	Moderate	Self	DR	IoT	Direct PDoS	Device Bricking

6. Discussion

The landscape of Permanent Denial of Service (PDoS) attacks is both diverse and continually evolving. While our work offers a comprehensive overview and classification of various PDoS attacks and vectors, there remain several challenges and future directions that the research community should focus on to provide effective countermeasures.

6.1. Challenges

Motivations and Economics: The motivations behind PDoS attacks are multifaceted and range from financial gains to political reasons. A deeper understanding of these motivations can offer insights into potential targets and the evolution of such attacks. Additionally, the underground economy that fuels the development and distribution of PDoS malware is a critical area that warrants investigation.

Systematic Characterization: The PDoS landscape is riddled with a multitude of malware families and variants. A systematic characterization and taxonomy that encapsulates all known strains can help in revealing patterns, shared characteristics, and, thus, potential vulnerabilities.

Evasion and Detection: Advanced PDoS malware often employs sophisticated evasion techniques, rendering traditional detection mechanisms ineffective. The potential of leveraging AI and machine learning for behavioral anomaly detection, especially in the context of such evasive tactics, is a promising area that needs exploration.

IoT Vulnerabilities: With billions of IoT devices getting integrated into our daily lives, their vulnerabilities become attractive targets for PDoS attacks. Given the resource constraints typical of IoT devices, devising lightweight yet effective detection and mitigation strategies is crucial.

Integration in Attacker Toolkits: How PDoS malware fits into broader attacker toolkits, frameworks, and intrusion kill chains remains an open question. Understanding this can provide insights into multi-stage attacks where PDoS is just one of the many goals.

Quantifying PDoS Severity: There's a pressing need for metrics that can quantify the severity and potential impact of PDoS attacks. Such metrics can guide response strategies, ensuring that the most damaging attacks are addressed with priority.

Addressing these challenges not only calls for innovative solutions but also opens up additional opportunities for future research, as shown in the following section.

6.2. Future Work

Collaborative Defense Strategies: As PDoS attacks evolve, so should our defense mechanisms. There is a potential in developing collaborative defense strategies, where insights from one domain (e.g., network security) can inform and bolster defenses in another (e.g., endpoint security).

Forensics and Attribution: Given the destructive nature of PDoS, post-attack forensics can be challenging. Developing robust forensic tools tailored for PDoS scenarios can not only help in understanding attack vectors but also in attributing attacks to specific threat actors.

Real-time Response Mechanisms: Exploring the design and implementation of real-time response mechanisms that can detect and mitigate PDoS attacks as they happen is a valuable direction. Such mechanisms can significantly reduce the potential damage of an attack.

User Education and Training: Many attacks, especially those that leverage social engineering and USB drives, can be thwarted with well-informed users. Future work can focus on developing training modules and awareness campaigns targeted at potential PDoS attack vectors.

Public Datasets: One of the challenges in researching PDoS attacks is the lack of comprehensive public datasets. Curating and releasing datasets that encapsulate various PDoS attack patterns can catalyze research in detection and mitigation strategies.

By addressing these challenges and focusing on the highlighted future work, we can pave the way for a more resilient digital ecosystem, safeguarded against the threats posed by PDoS attacks.

Metrics

There is a need for quantifiable metrics to measure various attributes of PDoS attacks, to enable more rigorous, data-driven analysis of these threats. Some potential PDoS attack metrics that could be developed through future research include:

- Attack Severity Index: A composite metric accounting for damage extent, recovery costs, denial duration (if applicable).

- Time-to-Failure: Measures duration between initial infection and total denial of service.
- Recovery Time Index: Quantifies time and costs to restore normal operations post-attack.
- Damage Range: Assesses scope of denial - whether localized to a subsystem or system-wide.
- PDoS Potency Vector: Multi-dimensional vector representing scores across relevant metrics.

By designing specific formulas to compute these quantifiable metrics based on attack attributes, we can enable data-driven PDoS analysis and informed mitigation prioritization. This represents a valuable direction for future research.

7. Conclusion

The undertaken research has confirmed that the permanent denial of service (PDoS) attacks represent an evolving and devastating cyber threat landscape. The thorough examination of the PDoS attacks allowed to deliver a comprehensive framework for their classification, that in its turn will become a solid ground for further research of PDoS attacks and development of holistic defense mechanisms.

The proposed taxonomy of the PDoS attacks, categorizing threats along multiple dimensions, brings much-needed structure to this expanding domain. By elucidating attack vectors, dissecting case studies, and delineating detection challenges, this work significantly advances conceptual clarity surrounding PDoS.

However, substantial gaps remain. Quantitative impact analysis and modeling PDoS severity could better inform defense prioritization. The motivations and ecosystem dynamics enabling PDoS development warrant deeper investigation. Tackling detection evasion tactics employed by advanced malware strains necessitates intelligent deception detection and AI-enabled behavioral anomaly identification.

Moreover, the proliferation of IoT escalates the need for PDoS solutions tailored to resource-constrained devices. Positioning PDoS within unified threat models and intrusion kill chains remains an open challenge. Ultimately, systematically quantifying the risk landscape is essential to appropriately calibrate defensive investments.

It is expected that this research will spur future work addressing the identified gaps. As PDoS threats increase in sophistication, leveraging ever-advancing attack toolkits, adaptive detection and timely recovery are paramount. Strategies like virtualization, micro segmentation, and real-time forensic analysis are the potential direction for both researchers and practitioners. The lasting resilience demands continuous innovation - in technology, tactics, and mindset - to counteract those intent on inflicting the permanent denial of service.

Appendix A

Appendix A.1. Killer Poke

- **Year of Discovery**: Late 1970s
- **Attack Vector**: Memory Interaction Command
- **Type**: Hardware
- **Complexity**: S (Simple)
- **Propagation Technique**: Manual
- **Payload Delivery Mechanism**: Direct Interaction
- **Targeted System**: Hardware (Monitor)
- **Category**: Direct PDoS
- **Impact**: Potential Monitor Damage

Appendix A.2. CIH/Chernobyl Virus

- **Year of Discovery**: 1998
- **Attack Vector**: Hardware Manipulation

- **Type**: Hardware
- **Complexity**: S (Simple)
- **Propagation Technique**: Manual
- **Payload Delivery Mechanism**: DD (Direct Download)
- **Targeted System**: Hardware
- **Category**: Direct PDoS
- **Impact**: Hardware Damage

Appendix A.3. TDL4 (TDSS/Alureon)

- **Year of Discovery**: 2007
- **Attack Vector**: Boot Process
- **Type**: Boot
- **Complexity**: C (Complex)
- **Propagation Technique**: Self
- **Payload Delivery Mechanism**: DD (Direct Download)
- **Targeted System**: Firmware
- **Category**: Extended PDoS
- **Impact**: Stealth Operation

Appendix A.4. BlackEnergy

- **Year of Discovery**: 2007
- **Attack Vector**: System Compromise
- **Type**: Multifaceted
- **Complexity**: C (Complex)
- **Propagation Technique**: Combo (Combination of Techniques)
- **Payload Delivery Mechanism**: DR (Dropper)
- **Targeted System**: ICS (Industrial Control Systems)
- **Category**: Extended PDoS
- **Impact**: Operational Disruption

Appendix A.5. Stuxnet

- **Year of Discovery**: 2010
- **Attack Vector**: System Compromise
- **Type**: Multifaceted
- **Complexity**: C (Complex)
- **Propagation Technique**: Combo (Combination of Techniques)
- **Payload Delivery Mechanism**: DR (Dropper)
- **Targeted System**: ICS (Industrial Control Systems)
- **Category**: Extended PDoS
- **Impact**: Operational Disruption

Appendix A.6. Olmasco

- **Year of Discovery**: 2011
- **Attack Vector**: Boot Process
- **Type**: Boot
- **Complexity**: M (Moderate)
- **Propagation Technique**: Manual
- **Payload Delivery Mechanism**: DR (Dropper)
- **Targeted System**: Firmware
- **Category**: Extended PDoS
- **Impact**: Stealth Operation

Appendix A.7. BrickerBot

- **Year of Discovery**: 2017
- **Attack Vector**: IoT Exploitation
- **Type**: IoT/Linux
- **Complexity**: C (Complex)
- **Propagation Technique**: Self
- **Payload Delivery Mechanism**: DD (Direct Download)
- **Targeted System**: IoT (Internet of Things)
- **Category**: Direct PDoS
- **Impact**: Device Bricking

References

1. Twist, J. Cyber Threat Reports 07 Mar-20 Mar 2017 **2017**.
2. Alashhab, Z.R.; Anbar, M.; Singh, M.M.; Hasbullah, I.H.; Jain, P.; Al-Amiedy, T.A. Distributed Denial of Service Attacks against Cloud Computing Environment: Survey, Issues, Challenges and Coherent Taxonomy. *Applied Sciences* **2022**, *12*, 12441.
3. Masters, G. Amnesia botnet targeting DVRs, Palo Alto report **2016**. https://www.scmagazine.com/amnesia-botnet-targeting-dvrs-palo-alto-report/article/649070/ Accessed: 2023-08-06.
4. Malik, M.; M.Léveillé, M.E. Meet Remaiten – a Linux bot on steroids targeting routers and potentially other IoT devices **2016**. https://www.welivesecurity.com/2016/03/30/meet-remaiten-a-linux-bot-on-steroids-targeting-routers-and-potentially-other-iot-devices/. Accessed: 2023-08-06.
5. Mamedov, O.; Sinitsyn, F.; Ivanov, A. Bad rabbit ransomware. *Retrieved May* **2017**, *1*, 2021.
6. Kharraz, A.; Robertson, W.; Balzarotti, D.; Bilge, L.; Kirda, E. Cutting the gordian knot: A look under the hood of ransomware attacks. In Proceedings of the International conference on detection of intrusions and malware, and vulnerability assessment. Springer, 2015, pp. 3–24.
7. Rodionov, D.E.; Matrosov, A.; Harley, D. Bootkits: Past, present and future. In Proceedings of the VB Conference, 2014.
8. Bhunia, S.; Hsiao, M.S.; Banga, M.; Narasimhan, S. Hardware Trojan attacks: Threat analysis and countermeasures. *Proceedings of the IEEE* **2014**, *102*, 1229–1247.
9. Alelyani, S.; GR, H.K. Overview of cyberattack on saudi organizations. *Journal of Information Security and Cybercrimes Research* **2018**, *1*, 32–39.
10. Ing-hau, C. CIH (Chernobyl) Malware. Unpublished, 1998. A malware created by Chen Ing-hau, a student at Tatung University in Taiwan. It affects only older Windows 9x (95, 98, Me) operating systems.
11. Fayi, S.Y.A. What Petya/NotPetya ransomware is and what its remidiations are. In Proceedings of the Information Technology-New Generations: 15th International Conference on Information Technology. Springer, 2018, pp. 93–100.
12. Khan, R.; Maynard, P.; McLaughlin, K.; Laverty, D.; Sezer, S. Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. In Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016 4, 2016, pp. 53–63.
13. Case, D.U. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)* **2016**, *388*, 3.
14. ICS-CERT. ICS Alert (IR-ALERT-H-17-102-01): BrickerBot Permanent Denial-of-Service Attack (Update A). https://www.cisa.gov/news-events/ics-alerts/ics-alert-17-102-01a, 2017.
15. Sachidananda, V.; Bhairav, S.; Elovici, Y. Spill the Beans: Extrospection of Internet of Things by exploiting denial of service. *EAI Endorsed Transactions on Security and Safety* **2019**, *6*.
16. Shobana, M.; Rathi, S. Iot malware: An analysis of iot device hijacking. *International Journal of Scientific Research in Computer Science, Computer Engineering, and Information Technology* **2018**, *3*, 2456–3307.
17. Matrosov, A.; Rodionov, E.; Harley, D.; Malcho, J. Stuxnet under the microscope. *ESET LLC (September 2010)* **2010**.
18. Marpaung, J.A.; Lee, H. Dark Seoul Cyber Attack: Could it be worse? In Proceedings of the Conf. Indonesian Stud. Assoc. in Korea, 2013.
19. Nissim, N.; Yahalom, R.; Elovici, Y. USB-based attacks. *Computers & Security* **2017**, *70*, 675–688.

20. Research, E. LOJAX - First UEFI rootkit found in the wild, courtesy of the Sednit group **2018**. https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf (visited on 11/19/2019).
21. Brierley, C.; Pont, J.; Arief, B.; Barnes, D.J.; Hernandez-Castro, J. PaperW8: an IoT bricking ransomware proof of concept. In Proceedings of the Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020, pp. 1–10.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.