Journal of
Cybersecurity and Privacy

MDPI

Article

Understanding and Classifying Permanent Denial-of-Service Attacks

Stanislav Abaimov

School of Computer Science, University of Bristol, Bristol BS8 1QU, UK; stanislav.abaimov@bristol.ac.uk

Abstract: In the evolving landscape of cybersecurity threats, 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 presents an in-depth exploration of PDoS attacks, emphasizing their distinguishing characteristics, underlying mechanisms, and potential further development. Through a comprehensive case study, this 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

check for updates

Citation: Abaimov, S. Understanding and Classifying Permanent Denial-of-Service Attacks. *J. Cybersecur. Priv.* **2024**, *4*, 324–339. https://doi.org/10.3390/jcp4020016

Academic Editor: Carlo Blundo

Received: 6 February 2024
Revised: 15 April 2024
Accepted: 29 April 2024
Published: 11 May 2024

1. Introduction

In today's dynamic cyber-threat environment, 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 and significant economic repercussions and, in 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 that resulted in billions of USD in global damages through the irreparable compromise of thousands of computers [1], there is significantly less dedicated research on PDoS attacks compared to its temporary counterparts [2]. This lack of systematic study leaves a deep gap in the scientific knowledge, while industries, governments, and individuals remain vulnerable to this specific threat.

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

Due to the limited number of malware cases that cause direct physical damage to devices, the scope of the literature review was expanded to include the cyber attacks that prevent devices from booting the operating systems and similar cases [3,4]. While the most widely used example of PDoS malware is BrickerBot [5], this research surveyed other known malware and malware strains, for example, TDL4 [3], StoneDrill [1], Mamba [6], Remaiten [7], Bad Rabbit [4], Silex, PaperW8 [8], and more.

The primary contributions presented in this paper are as follows:

1. A detailed exploration of PDoS attack vectors, evaluated with real-world case studies, including tactics like Internet of Things (IoT) exploitation [7,9], boot process disruption [4], and strategic data destruction [10].
2. The introduction of a novel classification framework for PDoS attacks, categorizing threats across dimensions such as damage mechanism, impact effect speed, target device and software, and recovery effort needed.
3. A severity score that allows the proposed classification to be applied in an accessible way.

Providing a systematic study of the PDoS attacks, this work also suggests future research directions to enable the development of specialized detection methodologies, informed mitigation plans, applications for incident response, and impactful metrics for quantifying PDoS repercussions. With increasing instances of PDoS attacks [6], this in-depth analysis is timely and of essential need 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, PDoS attacks target both software and hardware. These strategies extend beyond mere disruption, aiming to permanently disable the process.

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 [3], compromise the OS at the kernel level, making detection even more challenging.

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

- 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.

While the above are only techniques or even speculations, the following are specific real-world examples of cyber attacks that used unique attack vectors to prevent the functionality of the device:

- Stuxnet—ICS malware, kinetic impact;
- BrickerBot, NotPetya, PaperW8 [8]—wiper, corruption of storage;
- CVE-2022-23968 [11] —a reported vulnerability in Xerox VersaLink that, when exploited, sends device into a restart loop;
- Siemens ET200S nmap service scan—ICS malware, temporary shutdown of the Programmable Logic Controller.

The academic publications addressing PDoS (permanent denial-of-service) cyber attacks directly are limited, and this survey was carried out to address this gap. This survey included academic articles, whitepapers, and technical reports available from open public sources. The most widely used example is the malware BrickerBot [5], which has undergone considerable investigation, most notably in the study by Sachidananda et al. [12]. Their research offers an in-depth analysis of BrickerBot's capabilities, targeting methods, and potential impact. However, this research, as well as most of the analyzed studies, have a focus on a specific area and often lack a comprehensive holistic study of the entire attack type. PaperW8 [8] further studied IoT wiper techniques and presented a new malware.

Another gap in the current academic literature is the lack of consistent methodology for studying PDoS attacks. 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 [13,14].

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

3. 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 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.

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

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 [3], compromise the OS at the kernel level, making detection even more challenging.

3.1. Chernobyl (CIH Virus)

The CIH, also known as the Chernobyl Virus, emerged in 1998 as the first known hardware-targeting attack. CIH has the capability to overwrite system drive data and even attempt to flash the BIOS, rendering machines non-functional. This malware primarily targets PCs with the intent of direct hardware damage. The capacity to flash the BIOS is one of the unique approaches to causing PDoS and makes this the first known PDoS malware.

3.2. TDL4

TDL4, which emerged around 2007 as a sophisticated rootkit malware, representing a significant evolution in the PDoS threat landscape, is a specific strain of the Alureon banking trojan. While Alureon is a banking trojan that occasionally caused a Blue Screen of Death in 32-bit Microsoft Windows systems on a restart loop (power cycle), TDL4 malware is notable for its complex multi-component architecture and its ability to embed deeply within the host system, making detection and removal particularly challenging. TDL4, as a rootkit, primarily targets the boot process of a system by infecting the MBR to ensure its persistence and stealth.

The malware's advanced capabilities include kernel-mode rootkit techniques, encrypted communication with command and control servers, and a modular framework allowing it to download and execute additional payloads. TDL4 is also capable of dataflow manipulation, redirecting DNS requests, and performing man-in-the-middle attacks, thereby compromising the integrity of the system and the data passing through it.

Recovery from a TDL4 infection often requires specialized tools and techniques, as standard antivirus software struggle to effectively detect and remove the rootkit components. In some cases, the damage inflicted by TDL4's manipulation of system processes necessitates a complete system reinstallation or restoration from a clean backup.

3.3. StoneDrill

StoneDrill emerged in 2012. Distinctive for its destructive payload and advanced evasion techniques, StoneDrill infiltrates systems primarily through phishing attacks and exploits zero-day vulnerabilities. Once embedded, it employs a unique in-memory execution style. It injects malicious code directly into the memory of the browser process, making it particularly elusive. The malware's payload is centered on data encryption and deletion, specifically targeting and overwriting a variety of file types. Its design enables it to bypass administrative controls and access core system areas, leading to extensive data loss and system corruption. One of the notable technical feats of StoneDrill is its use of advanced obfuscation techniques, making the analysis and reverse engineering of its code a significant challenge for cybersecurity experts.

In effect, StoneDrill not only renders infected systems inoperable, but also necessitates comprehensive recovery efforts, often involving complete device replacement or extensive data recovery processes. Its impact is immediate and permanent, placing it among the more severe class of PDoS malwares.

3.4. Remaiten

Remaiten, identified in 2016, targets IoT devices, specifically Linux on embedded systems, primarily routers. It stands out for its strategy of exploiting IoT devices via remote access, primarily leveraging exposed telnet ports with weak authentication mechanisms.

After infecting the devices, Remaiten is able to perform system-level actions, download more malware on a device, and even scan and remove competing bots on a system compromised by it. In addition, this malware has the capability to disable the networking of the routers, rendering devices unusable until factory reset.

3.5. BrickerBot

BrickerBot, discovered in 2017, raised 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. Variations include BrickerBot.1, BrickerBot.2, BrickerBot.3, and BrickerBot.4.

BrickerBot's access method is to brute force the telnet password, then run commands using BusyBox to corrupt MMC and MTD storage, delete all files, and disconnect the device from the Internet. BrickerBot was specifically designed to compromise Linux-based IoT devices.

3.6. Silex

Emerging in 2019, Silex poses a significant threat to Linux systems and IoT devices with its multi-vector destructive capabilities. Its approach and shell commands are inspired, and some are directly borrowed from BrickerBot. After gaining root access, Silex corrupts system storage, wipes files, deletes firewall rules, and halts systems, rendering them non-functional. Silex targets both Linux systems and IoT devices, indicating an evolution in PDoS attack vectors. The malware leads to system-wide disruptions, often necessitating complete hardware replacements or reinstalls.

3.7. Mamba

Mamba, a unique ransomware variant, emerged with a distinct strategy of whole-disk encryption. Instead of encrypting individual files, Mamba encrypts entire hard drives, rendering systems inoperable. The malware is indiscriminate, targeting a wide range of systems, with the primary aim of data denial. Mamba's attacks lead to data inaccessibility, causing significant disruptions to affected entities.

3.8. Bad Rabbit

Bad Rabbit, a notable PDoS malware, was first detected in 2017, deploying a unique blend of ransomware and destructive attack tactics. It primarily infiltrates systems through a faux Adobe Flash installer on compromised websites, as a drive-by download. Upon execution, Bad Rabbit swiftly spreads across networks using a combination of hardcoded SMB credentials and the Mimikatz tool, which extracts login information from system memory.

Technically, Bad Rabbit was engineered to encrypt system files and the MBR, rendering the affected machines unbootable. This dual mechanism of attack, targeting both data and essential boot processes, distinguishes it from typical ransomware. The MBR encryption means that even if victims had backups of their data, the system itself requires significant remediation efforts, often involving complex recovery processes like complete OS reinstalls.

Moreover, Bad Rabbit stands out for its rapid propagation capability, echoing the behaviors of Petya/NotPetya, and its selective targeting of high-profile organizations and infrastructure. The malware's sophistication, including the use of legitimate tools for malicious purposes and its ability to cause widespread system disruptions, marks it as a formidable PDoS threat.

3.9. NotPetya

NotPetya [15], first detected in 2017, similarly diverges from typical ransomware. Technically, NotPetya combines aspects of ransomware with wiper malware, primarily targeting Microsoft Windows systems, leveraging "EternalBlue" for entry, and exploits the SMBv1 protocol vulnerability, as well as "Mimikatz", to extract credentials.

Once executed, NotPetya propagates within networks, overwrites the MBR, preventing normal boot processes, and then encrypts the Master File Table (MFT), rendering the file system unreadable. This dual-level encryption approach—targeting both the MBR and the MFT—is highly effective in denying access to the system without the decryption key. Despite presenting a ransom demand, NotPetya's design includes flaws in its payment and decryption system, leading researchers to classify it more as a wiper disguised as ransomware.

3.10. VPNFilter

VPNFilter, detected in 2018, is a multi-stage malware targeting routers and storage devices, including Linksys, MikroTik, Netgear, TP-Link, and QNAP. It includes a module, dstr, that renders infected devices inoperable. The dstr module, once executed, deletes files necessary for normal operation, including those associated with the malware itself, likely to obscure its presence during forensic analysis. It targets running processes related to VPNFilter and others for termination and then deletes various system files and directories. Significantly, it overwrites the bytes of all available /dev/mtdX devices with a 0xFF byte, erasing the flash memory. Finally, it executes a command to delete the remaining file system and reboots the device, leaving it unable to operate normally.

3.11. PaperW8

PaperW8 [8] is a malware designed to cause PDoS in IoT via remote access. It gains access to an IoT device through an exposed telnet port with weak authentication or utilizing an existing exploit, such as command injection. Once PaperW8 has gained access, its next aim is to upload its dependencies using tftp, commonly present in IoT devices. PaperW8 can kill any service that communicate with the user to prevent the device from being used. It will also kill any vulnerable services that were used to exploit the device, such that neither the user nor other attackers will be able to use the same vulnerability to regain access. Finally, PaperW8 will execute the uploaded binaries, taking full control of the device.

Finally, PaperW8 reads the bootloader partition into a buffer, encrypts it using AES-256-CBC, and then writes it back to the same partition, which will mangle the bootloader such that it will fail to boot if the device is restarted. This approach is similar to desktop-based ransomware that modify the MBR, such as Seftad and Petya. Affected devices include the following: HG532 Router (CVE-2017-17215 [16]), R6250 Router (CVE-2016-6277), MVPower DVR (using a backdoor shell), WiPG-1000 (CVE-2019-3929), 932L Camera (CVE-2019-10999), 5020L Camera (CVE-2019-10999).

The impact on the device is instant, as it does not require the encryption of the entire disk, and permanent, as it cannot be repaired without a full factory recovery or device replacement.

Table 1. Classification PDoS malware according to new framework.

Malware	**Year**	**Damage Mechanism**	**Impact Effect**	**Target Device**	**Target Software**	**Recovery Action**	**DoS Effect Duration**
Commodore PET's "Killer Poke"	1970s	Hardware damage	Instant	PC	Firmware	Device replacement	Temporary
CIH/Chernobyl Virus [17]	1998	Bootloader corruption	Fast	PC	OS	Device replacement	Permanent
TDL4 (TDSS/Alureon) [3]	2007	Data-flow manipulation	Instant	PC, ICS	Firmware, OS	Factory reset	Temporary
BlackEnergy [18,19]	2007	Data encryption/deletion	Fast	ICS	Control logic	Factory reset	Temporary
Stuxnet [20]	2010	Data-flow manipulation	Slow	ICS	Control logic	Physical restart	Temporary
Olmasco [3]	2011	Data-flow manipulation	Slow	PC, ICS	Firmware, OS	Factory reset	Temporary
Gapz [3]	2012	Bootloader corruption	Fast	PC	Firmware	Factory reset	rermanent
DarkSeoul [21]	2012	Data encryption/deletion	Instant	ICS	OS, Data	Device replacement	Temporary
StoneDrill [1]	2012	Data encryption/deletion	Instant	ICS	OS, Data	Device replacement	Permanent
Rovnix [3]	2014	Data-flow manipulation	Slow	PC	Firmware	Factory reset	Temporary
Mamba [6]	2016	Data encryption/deletion	Instant	PC, ICS	OS, Data	Factory reset	Permanent
Petya/NotPetya [15]	2016	Data encryption/deletion	Fast	PC	Firmware	Factory reset	Permanent
KillDisk [18,19]	2016	Data encryption/deletion	Instant	ICS	OS, Data	Device replacement	Temporary
Remaiten [7]	2016	Data encryption/deletion	Instant	IoT	Firmware	Factory Reset	Permanent
Amnesia [9]	2017	Data encryption/deletion	Instant	IoT	Firmware	Device replacement	Temporary

Table 1. *Cont.*

Malware	Year	Damage Mechanism	Impact Effect	Target Device	Target Software	Recovery Action	DoS Effect Duration
BrickerBot [5]	2017	Data encryption/deletion	Fast	IoT	Firmware	Device replacement	Permanent
Bad Rabbit [4]	2017	Bootloader corruption	Instant	PC	Firmware	Factory reset	Extended
USB Killer [22]	2017	Hardware damage	Instant	PC	-	Device Replacement	Permanent
LoJax [23]	2018	Bootloader corruption	Fast	PC	Firmware	Factory reset	Permanent
VPNFilter	2018	Data encryption/deletion	Instant	IoT	Firmware	Device Replacement	Permanent
MBRLock	2018	Bootloader corruption	Instant	PC	Firmware	Factory reset	Permanent
ZeroCleare	2019	Data encryption/deletion	Instant	ICS	OS, Data	Factory Reset	Temporary
Silex [8]	2019	Data encryption/deletion	Instant	IoT	Firmware	Device replacement	Permanent
PaperW8 [8]	2020	Bootloader corruption	Instant	IoT	Firmware	Factory reset/Device replacement	Permanent

3.12. CVE-2022-23968—Xerox VersaLink

A vulnerability in Xerox VersaLink devices was identified as CVE-2022-23968 [11]. The vulnerability allows remote attackers to brick these devices using a crafted TIFF file in an unauthenticated HTTP POST request, leading to a PDoS situation. The issue arises due to image parsing causing a reboot, which then restarts as soon as the boot process finishes, creating a loop. This can be resolved by a field technician.

3.13. Stuxnet

Stuxnet, in the context of this research, is a malware that created a change in the physics of the infected device, causing slow physical damage to the moving parts of the device by wearing them out. This malware was not designed to cause an immediate PDoS, while still managing to deliver irreversible damage.

4. Design of the Framework

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

The classification considers the PDoS attack's capability to disable devices through various means, including direct physical access, command execution, or system file manipulation. The following criteria were used for the proposed classification: damage mechanism, target device and target software, DoS effect duration, and recovery action.

The final proposed classification, presented in Figure 1, is as follows:

- Damage mechanism—bootloader corruption, data encryption/deletion, and data-flow manipulation;
- Impact effect—instant, fast, and slow;
- Target device—PC, IoT, ICS, and specific component;
- Target software—firmware, OS, data, and control logic;
- Recovery action—physical restart, factory reset, and device replacement.

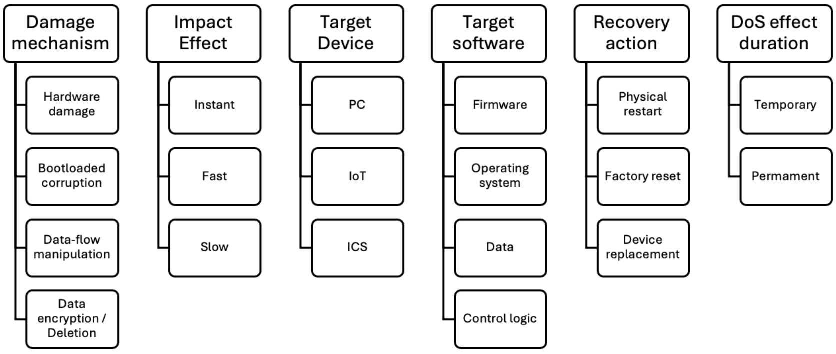

Figure 1. PDoS attack classification framework.

The summarized classification was applied to various examples of PDoS malware, as shown in Table 1 at the end of this section, while the detailed justification and breakdown of the distinct features are presented below.

4.1. Damage Mechanism

The damage mechanism describes the method used by the attacker to harm the target. From the case studies, several key damage mechanisms have been identified:

- Hardware Damage: This involves direct physical harm to hardware components. An example is the Commodore PET's "Killer Poke", which can cause monitor damage, and USB Killer.
- Bootloader Corruption: This targets the essential code required to launch the operating system. Malware like CIH/Chernobyl Virus and MBRLock exemplify this, potentially rendering devices inoperable.
- Data-flow Manipulation: This alters the way data are processed or transmitted within a system, leading to disrupted operations. Stuxnet and TDL4 are notable examples, demonstrating sophisticated interference with system processes.
- Data Encryption/Deletion: This involves rendering data inaccessible or permanently removing them. This can be seen in attacks like Mamba, where data encryption locks out legitimate users, or in instances of destructive malware like StoneDrill, which deletes critical files.

4.2. Impact Effect

The impact of an attack reveals its consequences. It can include device bricking, data inaccessibility, system compromise, and operational disruption, among others. However, the impact effect here is measured in the time that it takes for the damage to take the effect. Stuxnet is an example of an impact that takes a long time to damage the equipment, while in cases like those of USB Killer or PaperW8, the damage is almost instant. In cases like those of Petya and KillDisk, it takes time for the files to be encrypted before the system is damaged.

4.3. Target Device

This classification focuses on the target hardware of the attack. It could be hardware components, firmware, ICS, IoT devices, etc. Identifying the target helps in understanding the attacker's intent, whether it is to disrupt a specific process, damage hardware, or exploit a particular device type. It can also assist with developing incident response measures and financial impact estimates. For example, an expensive process-critical device without a fallback system can be a very valuable target for a PDoS attack.

4.4. Target Software

The "Target Software" category identifies the software components most vulnerable to a PDoS attack. This classification is critical, as it highlights the specific areas within a system where an attack could be most damaging and where in the system the defenses need to be deployed. It includes the following:

- Firmware: This essential software is often stored on non-volatile memory chips. Attacks on firmware can cripple the basic functionality of a device.
- Operating System: This core software manages computer hardware and software resources. Attacks targeting the OS can render a device inoperable.
- Data: Targeting stored data can lead to corruption or loss, significantly impacting device functionality and user access.
- Control Logic: In ICS and similar environments, attacking the control logic can disrupt operational processes, leading to extensive system damage.

There are certain cases of physical component damage, such as with a USB Killer, that would not affect software at all.

4.5. Recovery Action

PDoS attacks can be classified further into Direct PDoS and Extended PDoS attacks based on their lasting effects as follows:

- Physical Restart: the simplest form of recovery, often applicable in cases where the impact is minimal and temporary. Attacks causing temporary system unresponsiveness or minor disruptions typically fall under this category.
- Factory Reset: More severe attacks, leading to significant configuration or system changes that may require a factory reset. This involves restoring the system to its original state as defined by the manufacturer. While more time consuming than a physical restart, it can allow partial data recovery or at least the restoration of the device functionality.
- Device Replacement: The most extreme form of recovery. Device replacement is necessitated when the attack causes irreversible damage to the hardware or firmware, rendering the device unusable. This type of recovery is the most resource intensive, both in terms of cost and time. It is generally reserved for attacks of the highest severity, such as those causing permanent damage to critical components.

These distinctions help in understanding the longevity and potential repercussions of an attack, allowing for tailored response strategies.

4.6. DoS Effect Duration

The "DoS Effect Duration" classification in PDoS attacks characterizes the longevity of an attack's impact on the targeted system. The duration of an effect can be classified into two categories: temporary and permanent.

Temporary DoS Effect: Attacks classified under this category cause disruptions that, while potentially severe, do not inflict lasting damage on the system's hardware or software. Recovery actions typically involve system restarts, reconfigurations, or software reinstalls. The temporary nature of these attacks means that the core functionality of the hardware is retained post recovery. For instance, a malware like BlackEnergy, which temporarily disrupts ICS but can be resolved through device replacement, would fall under this category. Temporary DoS attacks, despite their reversible nature, can still have significant operational and financial repercussions.

Permanent DoS Effect: This category includes the most severe PDoS attacks, where the inflicted damage is irreparable, necessitating the complete replacement of the affected systems or components. Permanent attacks are often strategically planned and executed with the intent to cause irreversible damage to critical infrastructure or data. Malware like USB Killer, which physically damages the hardware, or PaperW8, which permanently corrupts the bootloader, create permanent DoS effects. Such attacks require extensive recovery efforts or full-device replacement.

4.7. Malware Evaluation Template

To systematically and uniformly assess the threat landscape of PDoS malware, a standardized template can be used to capture 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 the malware, ensuring a comprehensive evaluation. Each attribute in this template provides insight into the malware's nature, its potential impact, and the nuances of its design and deployment.

The malware evaluation template provides a structured approach to assessing and classifying 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 applied it to the known malware that have delivered PDoS attacks in the past.

4.8. 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 are 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, which causes 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, leverage 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.

4.9. PDoS Severity Score Based on Combined Criteria

Each PDoS malware or attack can be analyzed based on these criteria. The class it falls into provides a clear indication of its severity and the extent of response required. This multi-dimensional approach aims to offer a granular yet simplified understanding of the threat landscape and facilitates a targeted response strategy.

4.9.1. Class 1 (Minor)

Class 1 has the following characteristics:

- Impact Effect: Slow;
- DoS Effect Duration: Temporary;
- Recovery Action: Simple actions like physical restart or software update.

Class 1 represents the least severe category, characterized primarily by its less aggressive nature. This class encompasses attacks that induce a slow impact effect, resulting in temporary disruption that can often be rectified with basic corrective actions such as a physical restart or a standard software update. Examples within this class, such as Rovnix and Olmasco, demonstrate attacks that, while inconvenient, do not necessitate extensive recovery procedures. Class 1 PDoS attacks, therefore, while requiring vigilance, do not pose substantial long-term risks to the target systems, enabling quicker recovery and minimal impact on operational continuity.

4.9.2. Class 2 (Moderate)

Class 2 has the following characteristics:

- Impact Effect: Slow;
- DoS Effect Duration: Temporary or Permanent;
- Recovery Action: Factory reset or the reinstallation of software.

Class 2 in the spectrum of PDoS attacks is at a moderate level of threat. These attacks manifest with a slow impact effect but can lead to either temporary or permanent disruption. The distinguishing factor of Class 2 is the need for more intricate recovery actions compared to Class 1, such as factory resets or the complete reinstallation of software. This class includes malware instances like TDL4 and Petya, which represent a greater challenge in terms of mitigation and recovery due to their capacity to inflict lasting system changes or data losses. The attacks falling under this category might more deeply exploit ingrained system vulnerabilities or employ more complex attack methodologies, necessitating a deeper understanding of the affected systems for effective resolution. While not as immediately devastating as higher classes, Class 2 PDoS attacks underscore the importance of robust backup protocols and system resilience strategies. They act as a critical reminder of the need for regular system maintenance and updates to protect against evolving threats that can potentially cause prolonged downtime or significant data restoration efforts.

4.9.3. Class 3 (Significant)

Class 3 has the following characteristics:

- Impact Effect: Slow or Fast;
- DoS Effect Duration: Permanent;
- Recovery Action: More complex measures, potentially involving component replacements.

Class 3 in the spectrum of permanent denial-of-service (PDoS) attacks denotes a significantly higher level of threat compared to its lower-tier counterparts. This category is defined by attacks that deliver a slow or fast impact effect with permanent damage, necessitating advanced recovery methods often involving component replacements. Examples of Class 3 threats would include the CIH/Chernobyl Virus and MBRLock, which exhibit characteristics such as bootloader corruption, leading to substantial system disruption. Recovery from such attacks extends beyond simple resets or software reinstalls, demanding more resources and technical expertise.

The implications of Class 3 attacks are noteworthy in their capacity to cause lasting damage to systems, which may result in prolonged operational downtime or the permanent loss of critical data. The severity of these threats underscores the need for robust security measures and advanced preparedness plans. Class 3 PDoS attacks represent a sophisticated and dangerous class of malware, requiring immediate and specialized attention to mitigate and recover from their impacts. In the broader context of the PDoS threat landscape, these attacks highlight the evolving nature of cyber threats and the need for the continual adaptation of cybersecurity strategies.

4.9.4. Class 4 (Severe)

Class 4 has the following characteristics:

- Impact Effect: Fast or Instant;
- DoS Effect Duration: Permanent;
- Recovery Action: Involves extensive recovery efforts, such as major hardware overhauls.

Malware such as Mamba and StoneDrill can be classified as Class 4, where the extent of harm requires extensive recovery efforts, including major hardware overhauls or complete system restorations. The swift nature of these attacks, coupled with their irreversible damage, categorizes them as highly critical, demanding immediate and comprehensive response strategies.

At a technical level, a service scan of Siemens ET200S PLC can be classified as Class 4 PDoS attack, as it is instant, but temporary, and can be restored by a physical restart of the device.

4.9.5. Class 5 (Critical)

Class 5 has the following characteristics:

- Impact Effect: Instant;
- DoS Effect Duration: Permanent;
- Recovery Action: Full-device or full-system replacement.

Class 5 shows the most critical and destructive category of attacks. This class is characterized by its instantaneous impact effect and permanent damage, leading to dire consequences such as full system or device replacement. The profound severity of these attacks, exemplified by malware like USB Killer and PaperW8, showcases their capability to inflict irreversible damage to critical infrastructure or hardware. Such attacks often exploit deeply ingrained system vulnerabilities or deploy sophisticated techniques, leading to substantial financial and operational burdens. The recovery from Class 5 attacks is not only costly, but also complex, involving extensive resource allocation and potentially long-term operational downtime. The classification of an attack as Class 5 serves as a stark indicator of the highest level of threat, necessitating urgent attention and the mobilization of significant cybersecurity resources.

The benefits of using such an approach include comprehensive analysis, clear response guidelines, and strategic planning. Using this methodology, this classification becomes a tool for cybersecurity professionals and academic researchers to evaluate threats.

5. 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 we propose future directions that the research community should focus on to provide effective countermeasures.

5.1. Relevance and Lessons

The emergence of the CIH Virus, also known as Chernobyl, in 1998 created a paradigm shift in malware development. This was one of the first instances where malware was designed to directly target and cause irreversible damage to hardware components.

In 2017, BrickerBot brought a new wave of concerns as it thoroughly targeted the rapidly growing Internet of Things (IoT) ecosystem. This malware, known for its capacity to irreparably damage IoT devices, accentuated the critical need for enhanced security measures within this domain. BrickerBot underscored the importance of reinforcing IoT security through practices like changing default credentials, securing access points, and maintaining regular firmware updates. Silex, in 2019, highlighted the dynamic and constantly evolving landscape of PDoS threats. By targeting both Linux systems and IoT devices, Silex demonstrated a significant escalation in PDoS attacks.

Mamba, the upgraded version of Phobos ransomware, employs whole-disk encryption to render systems inoperable. As opposed to the standard file-specific encryption, data backup and recovery protocols, in the face of such sophisticated attacks, are needed.

The case of PaperW8 demonstrated the increasing complexity and ingenuity of PDoS attacks, especially in exploiting vulnerabilities within multiple IoT devices using the same malware. This malware's approach, involving multiple steps, from gaining access to executing destructive actions, illustrates the multifaceted nature of modern cyber threats. CVE-2022-23968 highlighted the vulnerability of even well-established hardware to PDoS attacks.

Collectively, these case studies not only enhance our understanding of the methodologies and impacts of various PDoS attacks, but also stress the imperative need for adaptive and forward-thinking cybersecurity strategies to protect against these continually evolving threats.

5.2. Potential Applications per Class

The proposed classification system for PDoS attacks, while not primarily defensive, serves critical roles in incident response and post-attack analysis. The classification system focuses on post-attack scenarios, providing a structured approach to understanding and mitigating the aftermath of PDoS attacks. This system is particularly crucial for organizations that are part of critical infrastructure, as it provides a methodology for dealing with such threats.

5.2.1. Damage Mechanism

In-depth analysis of the damage mechanism in PDoS attacks is pivotal for an effective system assessment, as it significantly influences the subsequent steps in incident management and recovery. A comprehensive understanding of the damage mechanism, whether it involves bootloader corruption, data encryption/deletion, or data-flow manipulation, directly shapes the strategic approaches used for system restoration and resilience. For instance, in cases where the bootloader is corrupted, the focus shifts to firmware-level interventions, which may include reflashing or reconfiguring firmware settings. On the other hand, data encryption or deletion necessitates a different set of recovery actions, potentially involving data recovery tools and techniques, or, in severe cases, resorting to backup systems for data restoration.

Knowledge of the damage mechanism also plays a crucial role in risk management and resource allocation during the recovery phase. By accurately gauging the impact and scope of the damage, organizations can prioritize their efforts and allocate resources more efficiently, ensuring a quicker return to normal operations. For critical infrastructure or high-value targets, this understanding is essential to minimizing operational disruptions and financial losses.

5.2.2. Impact Effect

The classification of the impact effect of PDoS attacks is a crucial element in shaping both immediate and strategic responses. This aspect of the classification determines the immediacy of the threat. In situations where the impact effect is instantaneous or fast, there is an immediate and clear threat to system integrity, which may take seconds to corrupt the system. These scenarios demand swift action to mitigate damage and prevent widespread system failure.

Conversely, PDoS attacks with slower impact effects present a different kind of challenge. These types of attacks may not immediately disrupt systems and instead gradually degrade performance or secretly compromise system integrity over time. The slower nature of these attacks often allows them to remain undetected for longer periods, potentially causing more insidious and widespread damage. Therefore, a thorough understanding of the impact effect is instrumental in developing long-term monitoring strategies. Continuous and proactive system monitoring becomes essential in these cases to detect and address these threats before they escalate into major incidents.

5.2.3. Target Device

The identification of the target device in PDoS attacks is a technical detail that aids in deploying a tailored and effective response by channeling resources toward the most critical and vulnerable systems. In incidents where multiple device types are affected, understanding the specific target devices helps in prioritizing actions based on their role and importance within the organization's infrastructure.

Knowing the target device is instrumental in shaping the response teams' approach, especially in environments with diverse technological ecosystems. For instance, an attack on an ICS would necessitate a different response strategy compared to an attack on general-purpose PCs or IoT devices. ICS attacks might require specialized knowledge and tools for mitigation and recovery, underlining the importance of having a team with the right expertise.

5.2.4. Target Software

The identification of target software—be it firmware, OS, data, or control logic—is instrumental in shaping both immediate recovery actions and long-term defensive strategies. From a scientific standpoint, this knowledge facilitates the selection of approaches to system recovery. For instance, attacks on firmware may require different recovery tools and approaches compared to those targeting OS layers. In cases of data-focused attacks, recovery might prioritize data decryption and restoration, often involving specialized software and techniques.

Additionally, the identification of the target software aids significantly in vulnerability assessment and management. It allows for a targeted analysis of existing vulnerabilities within similar systems or software components. This analysis is fundamental in the development of patches and updates, addressing specific vulnerabilities exposed by the PDoS attack. Such targeted updates are crucial in fortifying systems against similar future attacks, thereby enhancing the overall security posture.

5.2.5. Recovery Action

The significance of the "Recovery Action" classification in managing PDoS attacks extends far beyond immediate incident response. It is a comprehensive approach that influences strategic planning, resource allocation, and overall organizational preparedness in the face of cyber threats. Knowledge of a required recovery action contributes to the business operations, continuity, and risk management.

Detailed knowledge of the recovery action needed allows organizations to more accurately forecast recovery timelines and resource requirements. For instance, knowing that a PDoS attack necessitates full-device replacement versus a simple restart enables the targeted allocation of financial and technical resources.

Moreover, this classification aids in developing tailored training programs for IT staff and incident response teams. By understanding the spectrum of potential recovery actions, organizations can ensure that their teams are equipped with the necessary skills and tools to respond to a variety of scenarios. This preparation is crucial in reducing recovery time and mitigating the impact of attacks.

5.2.6. DoS Effect Duration

The duration of the denial-of-service effect is critical for business continuity planning. It aids organizations in assessing potential downtime and operational impact. Furthermore, for attacks resulting in permanent effects, this classification underscores the importance of investments in backups and redundant systems, which is essential for ensuring operational resilience and continuity in the face of such threats.

In summary, this multi-faceted classification system provides a comprehensive toolkit for addressing PDoS attacks, facilitating rapid response, effective recovery, and strategic planning for future incidents. Its application not only streamlines the response to current attacks, but also lays the groundwork for strengthening defenses against future PDoS threats.

5.3. Future Work and Potential Metrics

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

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

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.

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.

How PDoS classification 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.

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 on detection and mitigation strategies. This paper is the first step in developing a collection of features for such datasets.

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.

6. Conclusions

The undertaken research confirmed that permanent denial-of-service (PDoS) attacks represent an evolving and devastating cyber threat landscape. Their thorough examination allowed ua to develop a novel classification framework for PDoS attacks, categorizing threats across multiple dimensions, such as damage mechanism, impact effect speed, target device software, recovery effort needed, and DoS effect duration. In turn, this classifications can serve as solid ground for further research on PDoS attacks and the development of holistic defense mechanisms.

By explaining attack vectors, dissecting case studies, and breaking down the challenges, this work significantly advances conceptual clarity surrounding PDoS attacks. The proposed severity score facilitates the practical applicability of the framework.

However, substantial gaps remain. Defense prioritization requires an expanded quantitative impact analysis; the detection of advanced evasive malware strains requires intelligent intrusion detection and AI-enabled behavioral anomaly identification; IoT devices require Anti-PDoS solutions tailored to resource-constrained hardware. Positioning PDoS within unified threat models and intrusion kill chains remains an open challenge.

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, as well as edge-device intrusion detection systems, is a potential direction for both researchers and practitioners. Ultimately, systematically monitoring the risk landscape is essential to appropriately calibrating defensive investments. Lasting resilience demands continuous innovation—in technology, tactics, and mindset—to counteract those intent on inflicting permanent denial of service.

Funding: This research received no external funding.

Data Availability Statement: Data derived from public domain resources.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Twist, J. *Cyber Threat Reports 07 Mar–20 Mar 2017*; Army Cyber Institute: Fort Eisenhower, GA, USA, 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. *Appl. Sci.* **2022**, *12*, 12441. [CrossRef]
3. Rodionov, D.E.; Matrosov, A.; Harley, D. Bootkits: Past, present and future. In Proceedings of the VB Conference, Seattle, WA, USA, 24–26 September 2014.
4. Mamedov, O.; Sinitsyn, F.; Ivanov, A. *Bad Rabbit Ransomware*. 2021. Available online: https://securelist.com/bad-rabbit-ransomware/82851/ (accessed on 1 May 2017).
5. ICS-CERT. ICS Alert (IR-ALERT-H-17-102-01): BrickerBot Permanent Denial-of-Service Attack (Update A). 2017. Available online: https://www.cisa.gov/news-events/ics-alerts/ics-alert-17-102-01a (accessed on 6 August 2023).
6. Alelyani, S.; Kumar, H. Overview of cyberattack on saudi organizations. *J. Inf. Secur. Cybercrimes Res.* **2018**, *1*, 32–39. [CrossRef]

7. Malik, M.; Léveillé, M.E. Meet Remaiten—A Linux Bot on Steroids Targeting Routers and Potentially Other IoT Devices. 2016. Available online: https://www.welivesecurity.com/2016/03/30/meet-remaiten-a-linux-bot-on-steroids-targeting-routers-and-potentially-other-iot-devices/ (accessed on 6 August 2023).
8. Brierley, C.; Pont, J.; Arief, B.; Barnes, D.J.; Hernandez-Castro, J. PaperW8: An IoT bricking ransomware proof of concept. In Proceedings of the 15th International Conference on Availability, Reliability and Security, New York, NY, USA, 25–28 August 2020; pp. 1–10.
9. Masters, G. *Amnesia Botnet Targeting DVRs, Palo Alto Report*; CyberRisk Alliance: New York, NY, USA, 2016.
10. 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, Milan, Italy, 9–10 July 2015* ; Springer: Berlin/Heidelberg, Germany, 2015; pp. 3–24.
11. National Vulnerability Database. CVE-2022-23968—Xerox VersaLink Devices Vulnerability. Vulnerability in Xerox VersaLink Devices Allows Remote Attackers to Cause a Permanent Denial of Service via a Crafted TIFF File. 2022. Available online: https://nvd.nist.gov/vuln/detail/CVE-2022-23968 (accessed on 12 December 2023).
12. Sachidananda, V.; Bhairav, S.; Elovici, Y. Spill the Beans: Extrospection of Internet of Things by exploiting denial of service. In *EAI Endorsed Transactions on Security and Safety*; EAI: Gent, Belgium, 2019; Volume 6.
13. Shobana, M.; Rathi, S. Iot malware: An analysis of iot device hijacking. *Int. J. Sci. Res. Comput. Sci. Comput. Eng. Inf. Technol.* **2018**, *3*, 2456–3307.
14. Gulatas, I.; Kilinc, H.H.; Zaim, A.H.; Aydin, M.A. Malware Threat on Edge/Fog Computing Environments From Internet of Things Devices Perspective. *IEEE Access* **2023**, *11*, 33584–33606. [CrossRef]
15. 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, Chiang Mai, Thailand, 26–27 October 2018* ; Springer: Berlin/Heidelberg, Germany, 2018; pp. 93–100.
16. National Vulnerability Database CVE-2017-17215—Huawei HG532 Devices Vulnerability. Huawei HG532 with Some Customized Versions Has a Remote Code Execution Vulnerability. Successful Exploit Could Lead to the Remote Execution of Arbitrary Code. Available online: https://nvd.nist.gov/vuln/detail/cve-2017-17215 (accessed on 12 December 2023).
17. F-Secure Virus:DOS/CIH (Chernobyl) Malware. F-Secure Labs, 1999. Available online: https://www.f-secure.com/v-descs/cih.shtml (accessed on 14 December 2023)
18. 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, Belfast, UK, 23–25 August 2016; pp. 53–63.
19. Case, D.U. *Analysis of the Cyber Attack on the Ukrainian Power Grid*; Electricity Information Sharing and Analysis Center (E-ISAC): Washington, DC, USA, 2016; Volume 388, p. 3.
20. Matrosov, A.; Rodionov, E.; Harley, D.; Malcho, J. *Stuxnet Under the Microscope*; ESET LLC: San Diego, CA, USA, 2010.
21. Marpaung, J.A.; Lee, H. Dark Seoul Cyber Attack: Could it be worse? In Proceedings of the Conference Indonesian Student Association in Korea, Daejeon, Republic of Korea, 7 July 2013.
22. Nissim, N.; Yahalom, R.; Elovici, Y. USB-based attacks. *Comput. Secur.* **2017**, *70*, 675–688. [CrossRef]
23. ESET Research. *LOJAX—First UEFI Rootkit Found in the Wild, Courtesy of the Sednit Group*; ESET Research: San Diego, CA, USA, 2018.

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.