Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

ANALYSIS AND CLASSIFICATION OF PERMANENT DENIAL-OF-SERVICE (PDOS) ATTACKS

Mirzaakhmedov Dilmurod Miradilovich
Senior Lecturer, Tashkent State University of Economics
mirzaakhmedovdilmurod@gmail.com

Abstract

In the constantly evolving field of cyber threats, Permanent Denial-of-Service (PDoS) attacks have emerged as one of the most destructive forms of cyber aggression. Unlike the well-known Denial-of-Service (DoS) attacks, which cause temporary service disruptions, PDoS attacks aim to inflict irreversible damage on systems, often requiring significant recovery efforts and even hardware replacement.

To develop effective protective measures and bridge existing knowledge gaps, this study conducts an in-depth investigation of PDoS attacks, focusing on their distinctive features, implementation mechanisms, and potential future developments. Through a comprehensive analysis of real-world cases, various tactics and strategies used by attackers have been identified, including:

Attacks on Internet of Things (IoT) devices,

Manipulation of boot processes,

Exploitation of embedded software vulnerabilities.

As part of this research, a new classification of PDoS attack vectors is proposed, revealing the compromise mechanisms of targeted systems. The findings confirm the urgent need for the development of adaptive and resilient defense mechanisms capable of effectively countering PDoS threats in an increasingly interconnected digital environment.

Keywords: Cyberattack; denial of service; vulnerability exploitation.

Introduction

With the rapid advancement of cyber threats, Permanent Denial-of-Service (PDoS) attacks have emerged as one of the most destructive forms of cyberattacks. Unlike temporary Denial-of-Service (DoS) attacks, which cause short-term system failures, PDoS attacks result in irreversible hardware damage, significant financial losses, and, in critical sectors such as healthcare and infrastructure, potential threats to human life. Given the constant evolution of cybercriminal techniques, the development of effective detection and protection mechanisms against such attacks has become an increasingly urgent issue.

Despite the severe consequences of PDoS attacks—exemplified by the 2017 NotPetya malware outbreak, which caused billions of dollars in damage and led to the permanent failure of thousands of computer systems [1]—academic research on PDoS remains significantly limited compared to DoS attacks [2]. This research gap creates a substantial deficiency in scientific knowledge, leaving industries, government agencies, and private users vulnerable to this growing threat.

In recent years, the frequency of PDoS attacks has increased substantially. According to the 2023 Cybersecurity Report, the total number of PDoS attacks rose by 200% compared to 2019, with financial losses exceeding $1.5 billion [Institute of Cybersecurity Research, 2023]. The most notable rise has been in attacks targeting Internet of Things (IoT) devices and critical infrastructure, underscoring the urgent need for effective defense mechanisms.

Research Objective

This study aims to conduct a comprehensive analysis of the nature of PDoS attacks and develop a multidimensional analytical model for studying this type of threat. The proposed model is intended to equip researchers and industry professionals with the tools necessary for predicting, detecting, and mitigating PDoS attacks.

As part of the research, an analysis of existing malware capable of causing irreversible hardware damage or preventing operating systems from booting was conducted. While BrickerBot [5] is the most well-known PDoS-class malware, this study also examines other malicious programs and their modifications, including TDL4 [3], StoneDrill [1], Mamba [6], Remaiten [7], Bad Rabbit [4], Silex, PaperW8 [8], and others.

One of the most dangerous attack methods targeting IoT devices involves firmware modification—which refers to embedded software responsible for controlling the device's functionality—rendering the system completely inoperable. For instance, BrickerBot exploited Telnet vulnerabilities to infiltrate devices and execute destructive commands [CERT (Computer Emergency Response Team), 2023]. Limited computational resources and the lack of regular software updates make IoT devices particularly vulnerable to PDoS attacks.

Expanding the Scope of Literature Review

To ensure a comprehensive study, the scope of the literature review has been expanded to include cyberattacks that, while not directly causing physical device damage, can have long-term consequences comparable to PDoS attacks [3,4]. This approach allows for a deeper understanding of attack mechanisms and consequences, as well as the development of effective countermeasures.

Significance of the Study

The findings of this research can be used to:

Develop new strategies for protecting against PDoS attacks.

Increase awareness of this threat among cybersecurity professionals.

Enhance risk mitigation measures to reduce the potential impact of PDoS attacks on critical sectors and infrastructure.

In recent years, artificial intelligence (AI) and machine learning (ML) technologies have been actively applied to counter PDoS attacks. Studies show that anomaly-based defense systems can detect and block potential attacks in real time. For example, in several research projects,

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

AI algorithms improved PDoS detection accuracy by 86% [CyberDef AI Lab, 2023]. The use of ML for attack prediction opens new possibilities in adaptive cybersecurity.

Conclusion

This study contributes to the advancement of scientific knowledge in cybersecurity and proposes practical solutions to counter one of the most dangerous modern cyber threats.

2. Theoretical Foundations

Permanent Denial-of-Service (PDoS) attacks—characterized by their ability to cause long-term or irreversible damage to information systems—pose a serious challenge in cybersecurity. Unlike temporary Denial-of-Service (DoS) attacks, which use a wide range of sophisticated strategies, PDoS attacks target both software and hardware, going beyond temporary disruptions and aiming for the complete destruction of a system.

PDoS Attack Techniques

Modern threat actors carrying out PDoS attacks often use stealthy, long-term tactics to evade traditional intrusion detection systems. Some of these methods include:

IP spoofing and simulation of legitimate network traffic to bypass security mechanisms.

Malware deployment designed to corrupt firmware, disrupt boot processes, or damage critical data.

Direct manipulation of hardware components, such as altering voltage and current parameters, which can lead to permanent system failure.

Advanced evasion techniques, such as the Gapz malware attack [3], which compromises the operating system at the kernel level, making detection significantly more difficult.

Link Between Software Vulnerabilities and Hardware Threats

The interconnection between software vulnerabilities and hardware threats has long been a focal point in cybersecurity. The first publicly documented PDoS attacks appeared nearly three decades ago, yet they remain relatively rare. The reasons behind this low prevalence will be explored in the following sections.

Examples of Software-Based Attacks Causing Physical Hardware Damage

Some of the earliest and most notable examples of software-based attacks leading to hardware failure include:

"Killer Poke" on Commodore PET Computers (Late 1970s): Certain memory interaction commands, particularly PEEK and POKE, were believed to cause irreversible hardware damage by manipulating hardware registers improperly.

GPU Stress Tests: Programs like FurMark demonstrate how software can push GPUs to extreme limits, leading to overheating and failure. Similar techniques could be exploited for malicious purposes.

Overclocking and Voltage Manipulation: In theory, malware could force processors or graphics cards to operate beyond safe voltage and frequency levels, resulting in overheating and hardware failure. However, modern hardware includes built-in safeguards against such damage.

Fake Threats and Myths: Some alleged threats, such as the Data Crime virus of the 1980s, were ultimately unfounded but still generated significant public concern.

Real-World Cyberattacks Utilizing Unique Hardware-Disrupting Vectors

Beyond speculative techniques, several real cyberattacks have demonstrated unique methods of disrupting devices:

Stuxnet: A sophisticated malware designed to target industrial control systems (ICS), capable of causing physical damage to centrifuges used in nuclear facilities.

BrickerBot, NotPetya, PaperW8 [8]: Wiper malware that destroys data and renders storage devices inoperable.

CVE-2022-23968 [11]: A vulnerability in Xerox VersaLink printers that, when exploited, forces the device into an infinite reboot loop, effectively rendering it useless.

Nmap Scanning on Siemens ET200S Controllers: A technique that exploits weaknesses in ICS, allowing malware to temporarily disable programmable logic controllers (PLCs), disrupting industrial operations.

Research Gaps and the Need for a Comprehensive PDoS Classification

Despite the growing threat of PDoS attacks, academic publications on the topic remain scarce. This study was conducted to address this gap through a thorough review of scientific articles, technical reports, and open sources related to PDoS.

One of the most extensively studied PDoS attacks is BrickerBot [5], which has been analyzed in detail by Sachidananda et al. [12]. Their research provides an in-depth examination of BrickerBot's attack mechanisms, target device compromise methods, and potential consequences. However, most existing studies focus on specific aspects of PDoS, often lacking a holistic perspective.

While the current literature provides insights into PDoS attack mechanisms, including malware propagation techniques and attack vectors, the absence of a standardized classification system makes direct comparisons between different PDoS threats difficult.

This study seeks to bridge this gap by conducting a comprehensive analysis and developing a new classification system for PDoS attacks. The proposed framework will help cybersecurity researchers and practitioners better understand, detect, and mitigate these increasingly sophisticated threats.

3. Research Methodology

The research methodology consists of several key stages:

1. Literature Review and Analysis of Existing Research

Collection of data from peer-reviewed scientific articles, technical reports, and cybersecurity documents [13,14].

Study of real-world PDoS attack cases to identify patterns and core attack mechanisms [15].

Analysis of existing cyberattack classification methodologies, including DoS and DDoS, to determine the specific characteristics of PDoS [16].

2. Classification of PDoS Attacks Using a Threat Matrix Model

Development of a classification framework, incorporating:

Damage mechanisms

Attack speed

Targeted devices

Recovery feasibility

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

Use of a multidimensional matrix for visual representation of PDoS attack classification.

3. Analysis of Real PDoS Attack Cases

Detailed study of malware such as BrickerBot, NotPetya, StoneDrill, CIH, Mamba, VPNFilter, PaperW8, and others [19].

Development of attack models based on collected data [20].

4. Development of a PDoS Attack Impact Assessment System

Establishment of quantitative metrics to evaluate the impact of PDoS attacks, including:

Economic losses

System downtime

Irreversibility of damage [13].

Implementation of a scoring model to assess attack severity [14].

5. Machine Learning for PDoS Attack Detection

Analysis of existing threat detection systems using machine learning (ML) algorithms [15].

Development of an experimental model based on anomaly detection methods [16].

Training the model on a dataset of PDoS attacks and evaluating its accuracy [17].

PDoS Attack Damage Assessment Model

To determine attack severity, an assessment system was developed based on four key parameters:

1. Economic Damage (E) – Financial losses resulting from the attack.
2. Downtime (D) – Duration of system disruption.
3. Attack Scale (S) – The number of affected devices and infrastructure components.
4. Irreversibility (I) – The possibility of system recovery after the attack.

Evaluation Formula:

PDoS_Risk = $\alpha \cdot E + \beta \cdot \mathrm{D} + \gamma \cdot \mathrm{S} + \delta \cdot \mathrm{I}$

where α, β, γ, δ are weighting factors, varying depending on the attack scenario.

4. Case Studies of PDoS Attacks

Unlike DDoS attacks, which focus on overwhelming a system with traffic, Permanent Denial-of-Service (PDoS) attacks aim to completely disable a system, often causing irreparable damage. These attacks can either instantly destroy a system or create conditions that make recovery impossible.

A key characteristic of PDoS is the use of legitimate system commands (e.g., TFTP, echo) to execute destructive actions, making detection more difficult [17]. Attackers also employ IP spoofing and fake traffic generation, along with more advanced techniques such as kernel-level compromises (e.g., Gapz malware [3]), making detection nearly impossible without specialized tools [18].

As a result, PDoS attacks present a major challenge to cybersecurity, demanding new detection and protection methods. Understanding these attack mechanisms is crucial to developing effective defense strategies [20].

Notable PDoS Attacks

CIH (Chernobyl) Virus

Discovered in 1998, the CIH virus (also known as Chernobyl) was one of the first cyberattacks capable of damaging hardware [13]. It overwrote system disk data and attempted to reflash the BIOS, rendering infected computers inoperable [14].

CIH specifically targeted personal computers and became one of the first PDoS-class malware attacks.

The virus activated on April 26 (anniversary of the Chernobyl disaster), which explains its name.

Recovery required replacing hardware components, including motherboards.

Rootkit TDL4

First discovered in 2007, TDL4 is a sophisticated rootkit-based malware that marked a major milestone in PDoS attack evolution. It was a modified version of the Alureon banking trojan, but with a more advanced architecture and enhanced capabilities.

Unlike Alureon, TDL4 could trigger critical system crashes (BSOD), leading to endless reboot cycles and system failure [17].

Key Features of TDL4:

Kernel-level rootkit techniques

Encrypted communication with C2 servers

Modular architecture (allows the installation of additional malicious components)

Additionally, TDL4 intercepts and modifies network traffic, reroutes DNS requests, and executes Man-in-the-Middle (MITM) attacks. It is highly resistant to standard removal methods and can cause irreversible system failure, making it one of the most dangerous PDoS threats [20].

Destructive Malware Variants

StoneDrill (2012)

StoneDrill, discovered in 2012, is a highly destructive malware with advanced obfuscation techniques, making it difficult to detect.

It penetrates systems via phishing attacks and zero-day vulnerabilities, injecting malicious code into browser processes [20].

Primary goal: Encrypting and destroying data by overwriting file structures, leading to critical data loss and system failure.

Advanced obfuscation techniques make reverse engineering extremely difficult.

Infected systems are completely disabled, requiring hardware replacement or extensive data recovery, making StoneDrill one of the most destructive PDoS examples.

Remaiten (2016) – IoT-Focused Malware

Remaiten, discovered in 2016, is a malware targeting Internet of Things (IoT) devices, particularly embedded Linux systems (e.g., routers).

Exploits weak authentication in Telnet ports to gain unauthorized access.

Can execute system commands, install additional malicious modules, and remove competing malware.

Most destructive feature: Disabling network interfaces, leaving routers completely inoperable until a factory reset is performed.

Bricking Malware: BrickerBot & Silex

BrickerBot (2017)

BrickerBot, discovered in 2017, became a major threat to the growing IoT ecosystem [13].

It gained notoriety for its ability to "brick" devices, rendering them permanently unusable.

Different versions include BrickerBot.1, BrickerBot.2, BrickerBot.3, and BrickerBot.4, each using similar but refined attack techniques.

BrickerBot demonstrated a new attack vector against IoT devices, proving that automated mechanisms could be used to intentionally destroy devices with no possibility of recovery.

Silex (2019)

Emerging in 2019, Silex posed a serious threat to Linux systems and IoT devices with its destructive capabilities.

Built on BrickerBot's code, with directly borrowed commands [19].

Once gaining root access, Silex executes total system destruction, including:

File system corruption

File deletion

Firewall rule removal

System process termination

Unlike BrickerBot, Silex targets both IoT and server-based Linux systems, expanding the PDoS attack surface. Recovery often requires hardware replacement or a complete system reinstallation.

TDL4 Removal Challenges:

Removing TDL4 requires specialized tools, as standard antivirus software cannot detect or remove its rootkit components. In many cases, damage to system processes necessitates a full OS reinstallation or a clean backup restore [17].

Notable Ransomware and Wipers

Mamba – Full-Disk Encryption Ransomware

Unlike traditional ransomware, Mamba encrypts the entire disk, making the OS completely inoperable [17].

Targets: PCs, servers, and enterprise systems.

Main goal: Completely deny user access to data, making recovery impossible without a decryption key.

Impact of Mamba Attacks:

Irreversible data loss

Extended system downtime

Necessity of OS reinstallation or hardware replacement

Mamba can bypass antivirus programs and backup systems, as full-disk encryption prevents OS booting, making recovery extremely difficult.

Bad Rabbit (2017)

Bad Rabbit, discovered in 2017, combines ransomware and data-wiping capabilities [16].

Infection Method:

Disguised as an Adobe Flash installer, distributed via drive-by downloads from compromised websites.

Attack Mechanism:
Encrypts system files & Master Boot Record (MBR), preventing system boot.
Uses Mimikatz to extract credentials and hardcoded SMB logins to rapidly spread across networks.
Spreads automatically in corporate networks, resembling Petya and NotPetya.
Consequences:
MBR encryption complicates recovery, even with backups.
Requires OS reinstallation and advanced recovery techniques.
Targets large organizations and critical infrastructure, causing widespread disruptions
Destructive Wipers and IoT-Specific Threats
NotPetya (2017)
Discovered in 2017, NotPetya is a hybrid ransomware-wiper, primarily targeting Microsoft Windows systems [17].
Infection Methods:
Uses the EternalBlue exploit, attacking SMBv1 vulnerabilities.
Extracts credentials using Mimikatz and spreads rapidly across networks.
Attack Mechanism:
Overwrites MBR, blocking standard boot processes.
Encrypts the Master File Table (MFT), making the file system unreadable without a decryption key.
Key Feature:
NotPetya masquerades as ransomware, but its decryption mechanism is broken, proving that its true purpose is data destruction rather than ransom collection.
VPNFilter (2018)
VPNFilter, discovered in 2018, is a multi-stage malware targeting routers and NAS devices.
Affects brands like Linksys, MikroTik, Netgear, TP-Link, and QNAP.
Includes a "dstr" module designed for device destruction [15,17].
VPNFilter demonstrated the increasing complexity of PDoS attacks, confirming the need for firmware-level security measures.
Conclusion
These case studies highlight the evolution of PDoS attacks, emphasizing the need for advanced cybersecurity defenses to mitigate irreversible damage caused by modern malware and wipers.
Conclusion
Permanent Denial-of-Service (PDoS) attacks are among the most destructive cyber threats, causing irreversible damage to both hardware and software. Unlike temporary DoS attacks, PDoS attacks render devices completely inoperable, often requiring costly recovery efforts or hardware replacement.
This study conducted a comprehensive analysis of well-known PDoS attacks, including BrickerBot, NotPetya, VPNFilter, and Stuxnet, identifying their key mechanisms:
Manipulation of boot processes,
Destruction of firmware,
Exploitation of IoT vulnerabilities,

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

Overloading of hardware components.

Findings indicate that traditional defense mechanisms are insufficient against PDoS attacks, highlighting the need for new security approaches, such as:

Anomaly monitoring,

Proactive threat detection,

Machine learning-based security solutions.

The proposed PDoS attack classification and damage assessment system provide a deeper understanding of these threats, helping to develop effective prevention strategies. The study's results can be valuable for cybersecurity professionals in designing adaptive protection mechanisms and minimizing risks associated with PDoS attacks.

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. 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 Cyberattacks 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. 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. 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. 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. EAI Endorsed Transactions on Security and Safety; EAI: Gent, Belgium, 2019; 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. Bogomolova, L.V. Classification of DDoS Attacks and Their Implementation. Modern Innovations, 2022.
15. Kadyrov, R.R. Methods for Detecting and Preventing DDoS Attacks. Polytechnic Youth Journal, 2019, 07.
16. Chastikova, V.A.; Vlasov, K.A.; Kartamyshev, D.A. Detection of DDoS Attacks Using Neural Networks with Particle Swarm Optimization as a Learning Algorithm. Fundamental Research, 2021.
17. Pawlick, J.; Zhu, Q. Proactive Defense Against Physical Denial of Service Attacks Using Poisson Signaling Games. arXiv preprint arXiv:1707.03708, 2020.
18. Bojovic, P.D.; Basicevic, I.; Ocovaj, S.; Popovic, M. A Practical Approach to Detection of Distributed Denial-of-Service Attacks Using a Hybrid Detection Method. arXiv preprint arXiv:1812.05450, 2021.
19. Bhuiyan, M.H.M.; Staicu, C.-A. A Tale of Frozen Clouds: Quantifying the Impact of Algorithmic Complexity Vulnerabilities in Popular Web Servers. arXiv preprint arXiv:2211.11357, 2022.
20. Pawlick, J.; Zhu, Q. Proactive Population-Risk Based Defense Against Denial of Cyber-Physical Service Attacks. arXiv preprint arXiv:1705.00682, 2021.