Astana IT University

SHERKHAN ZHUNUSBAY
NURBEK KYDYRALIEV
ASANALI TAZHIGALIYEV

Research on recent exploitation of zero-day vulnerabilities and analysis of techniques and methodologies used by attackers

6B06301 - Cybersecurity

Diploma work

Supervisor
Nurmukhanbetoba A.
Master of Technical Sciences, Teacher

Kazakhstan Republic
Nur-Sultan, 2024

CONTENTS

DEFINITIONS

Following terms are used in this work:

Term	Zero Day Attack
Term title	Research on recent exploitation of zero-day vulnerabilities and analysis of techniques and methodologies used by attackers
Terminology	Zero-day attacks, a critical concern in cybersecurity, exploit vulnerabilities not yet known to developers or security teams. These attacks occur in the lapse between the discovery of a vulnerability and the deployment of a patch, offering attackers a golden opportunity to inflict damage or steal data. Zero-day exploits thrive in secrecy, capitalizing on the delay in vulnerability acknowledgment and remedy. Zero-day vulnerabilities serve as hidden doors for attackers, allowing them to launch assaults on systems, compromise sensitive information, or disrupt essential services without prior detection. The race against time to identify and mitigate these vulnerabilities underscores the ongoing battle between cybersecurity professionals and attackers, with the former constantly developing strategies to predict and counteract threats before they manifest.

DESIGNATIONS AND ABBREVIATIONS

Following designations and abbreviations are used in this work:

$\forall$	text
AAA	text text text.
ABC	text text text text text text text text text text text text text text text text text.

INTRODUCTION

Work relevance. The relevance of this topic is underscored by the growing complexity of cyberattacks and the increasing reliance of society on digital infrastructure for critical services, including finance, healthcare, and government operations. The exploitation of zero-day vulnerabilities poses a significant risk to national security, corporate integrity, and personal privacy, making the study of these attacks not just a technical necessity but a societal imperative. By dissecting recent incidents and analyzing attacker methodologies, this research aims to shed light on the current landscape of cyber threats and contribute to the development of more effective defense mechanisms.

Goal of the work. The main aim of this investigation is to delve deeply into the realm of zero-day vulnerabilities' exploitation, shedding light on the tactics and methods attackers employ. Through this exploration, we seek to discern patterns and trends within these cyber onslaughts, offering rich insights into the shifting sands of cybersecurity threats. Grasping the nuances of zero-day exploit techniques is crucial for informing the crafting of sturdier security measures and defense mechanisms, aiming to shield against forthcoming vulnerabilities.

Research object. We set our sights on the exploitation of zero-day vulnerabilities spanning various realms, such as government, defense, tech, finance, consumer electronics, and web services. This includes probing into the vulnerabilities themselves, the scenarios under which they are exploited, the attackers' profiles, and the aftermath of these cyber intrusions.

Novelty. What sets this study apart is its razor-sharp focus on recent zero-day exploits, especially those emerging in the past few years. Moving beyond the general overview offered by earlier studies, our research zooms in on the specifics of current zero-day exploit techniques and the distinct challenges they pose. We aim to weave together disparate incidents to offer a unified understanding of how attackers' methods are morphing. Moreover, this investigation is poised to unveil fresh defensive insights, suggesting new security tactics grounded in the identified patterns and trends.

Research methodology. Our methodology is a blend of qualitative and quantitative analyses, embracing a thorough literature review, content analysis of various reports and publications, comparative analysis to pinpoint attack technique patterns, and a framework for gauging the impact of zero-day exploits. Interviews with cybersecurity mavens will further enrich our findings, embedding practical wisdom into our proposed defense strategies.

Practical relevance of the work. The practical implications of our findings are wide-ranging, catering to the needs of cybersecurity experts, decision-makers, and software crafters alike. For cybersecurity squads, the unveiled attacker methodologies could pave the way for more potent detection and response

maneuvers. Decision-makers might find the insights pivotal for understanding zero-day exploits' broader impacts on national security and economic health, potentially steering cybersecurity policies and legislation. Software developers and tech firms could harness this knowledge to fortify their security protocols, emphasizing vulnerability management and secure coding practices. By aiming to fortify the digital landscape, this research endeavors to bolster our collective defense against zero-day vulnerabilities' exploitation.

Objectives:

1 Identifying and cataloging recent zero-day vulnerabilities is the initial step. This involves creating an exhaustive list of zero-day vulnerabilities identified and exploited over the last few years. The catalog will detail the nature of these vulnerabilities, the software or systems impacted, the contexts in which these vulnerabilities were exploited, and the outcomes of these exploits. Understanding the extent and magnitude of the challenge that zero-day exploits represent is crucial, making this objective a foundational element of the study.

2 Analyzing attack techniques and methodologies stands as the second goal. This objective delves into the strategies and methods attackers use to exploit zero-day vulnerabilities. It encompasses the examination of initial access vectors, exploitation techniques, post-exploitation activities, and the attackers' ultimate goals. By scrutinizing these elements, the study aims to identify patterns in attacker behavior and methodologies, providing insights into how future zero-day exploits could be carried out and, possibly, thwarted.

3 Developing recommendations for mitigation and defense strategies is the concluding objective. Drawing from the insights obtained through the analysis of zero-day exploits and attacker methodologies, this goal involves formulating practical recommendations to bolster cybersecurity defenses against zero-day vulnerabilities. These suggestions are intended for a wide array of stakeholders, including software developers, cybersecurity practitioners, and policymakers, emphasizing the enhancement of detection capabilities, response preparedness, and overall resilience to such threats.

Literature review: In the evolving landscape of cybersecurity, recent research has illuminated the multifaceted approaches attackers employ to exploit zero-day vulnerabilities, reflecting both the complexity of cyber threats and the innovative strides in defense mechanisms. This segment of the literature review delves into these dynamics, presenting key findings from recent scholarly contributions.

1 Exploration of Exploitation Techniques: Singh, Joshi, and Kanellopoulos (2019) delve into the intricacies of how attackers leverage vulnerabilities within networked applications. Their study underscores the inherent challenges in identifying zero-day vulnerabilities, given their previously unknown status.

They propose a novel detection and prioritization framework, rooted in probabilistic analysis, aiming to enhance the early identification of such vulnerabilities.

2 Innovations in Defense Mechanisms: Al-Rushdan et al.'s work in both 2019 and 2020 introduces cutting-edge detection and prevention strategies tailored for Software-Defined Networks (SDNs). By adapting the Cuckoo sandbox tool, their research demonstrates significant advancements in thwarting zero-day malware attacks, effectively isolating infected clients to mitigate broader network compromise.

3 Advancements in Detection Methodologies: Wangde et al. (2021) propose an outlier-based detection model, trained on both benign and known malicious traffic, to identify anomalous, potentially harmful activity. This model has shown promising results in pinpointing unknown attacks, offering a significant leap forward in detecting specific types of cyber threats with high accuracy.

4 Comprehensive Risk Assessment Techniques: The work of Ye, Guo, and Ju (2019) introduces a comprehensive framework for assessing the risk associated with zero-day vulnerabilities and potential attack paths. Their methodology provides a multi-dimensional quantitative risk evaluation, enhancing the understanding of the implications of such vulnerabilities.

5 Utilization of GANs for Malware Detection: Peppes et al. (2023) explore the potential of Generative Adversarial Networks (GANs) in generating synthetic datasets of zero-day attack data. This approach aims to enrich the training and evaluation of Neural Network classifiers, with preliminary findings indicating that synthetic data can significantly improve model efficacy in detecting zero-day attacks.

These studies collectively underscore the nuanced and evolving nature of zero-day attacks, highlighting the critical need for innovative detection and prevention mechanisms. The research not only illuminates the diversity of methodologies employed by attackers but also showcases the potential of machine learning and artificial intelligence in crafting more resilient cyber defense strategies.

1 The analysis of recent zero-day vulnerabilities exploited in the wild reveals several key findings from the latest research.

1.1 Identification of Zero-Day Vulnerabilities

Zero-day attacks give developers no time to patch vulnerabilities before exploitation, highlighting the crucial need for proactive defense mechanisms and rapid response strategies to minimize damage ([Madou, 2022]

The increasing number of Zero Day Threats (ZDTs) underscores the importance of robust AI-based detection models capable of identifying novel threats in real-time by analyzing network flow telemetry and asset-level graph features ([Redino et al., 2022]

1.2 Technical Details and Impact

The Log4shell vulnerability demonstrates the profound impact zero-day vulnerabilities can have on the global cybersecurity landscape, with companies struggling to mitigate the threat through patches or security measures ([Everson et al., 2022]

Approaches like PlausMal-GAN for generating plausible malware data suggest innovative ways to enhance detection of zero-day malware by learning from generated analogous malware data, indicating a shift towards proactive and predictive cybersecurity strategies ([Won et al., 2023]

1.3 Methodologies for Exploitation

The use of Generative Adversarial Networks (GANs) to generate synthetic zero-day attack data for training neural network classifiers highlights a novel approach to improving detection rates of such vulnerabilities by incorporating realistic, yet synthetic, attack scenarios into the training process ([Peppes et al., 2023]

Semi-supervised machine learning approaches, leveraging the law of anomalous numbers (Benford's law), show promise in identifying significant features indicative of zero-day attacks, thus enhancing the detection capabilities of network intrusion detection systems ([Mbona and Eloff, 2022]

1.4 Preventive Measures and Response Strategies

The integration of threat intelligence platforms with existing security systems has been identified as a pivotal factor in enhancing preemptive security measures. These platforms facilitate the real-time sharing of threat data among organizations, enabling quicker identification and mitigation of zero-day exploits before they can cause widespread damage ([Kumar and Singh, 2023]).

The adoption of blockchain technology for securing software supply chains presents a novel approach to preventing zero-day attacks. By ensuring the integrity and authenticity of software components, blockchain can significantly reduce the

risk of introducing vulnerabilities that could be exploited by attackers ([Chen et al., 2023]).

1.5 Regulatory and Policy Implications

There is a growing consensus on the need for more stringent regulatory frameworks to mandate the disclosure of zero-day vulnerabilities. Such policies could incentivize companies to promptly report and address vulnerabilities, thereby reducing the window of opportunity for attackers to exploit these flaws ([Jackson and Tylor, 2022]).

International collaboration and information-sharing agreements between governments and private sectors have been highlighted as crucial in combating the global threat posed by zero-day vulnerabilities. These partnerships can lead to the development of more robust and universally applicable cybersecurity measures ([Patel and Wei, 2023]).

1.6 Future Directions in Cybersecurity Research

The exploration of quantum computing as a double-edged sword in the realm of cybersecurity poses an interesting future challenge. While it offers the potential for creating nearly unbreakable encryption, it also could enable the development of tools capable of decrypting current cryptographic protections, necessitating preemptive research into quantum-resistant cybersecurity measures ([Li and Zhang, 2023]

The potential for AI-driven autonomous security systems that can adapt and respond to threats in real-time is being closely examined. Such systems would represent a significant leap forward in proactive cybersecurity, capable of not just detecting, but also autonomously mitigating threats without human intervention ([D'Souza and Rajan, 2023].

In synthesizing these insights, it becomes evident that the battle against zero-day vulnerabilities is evolving rapidly, with technological innovation at its core. The emphasis on AI and machine learning, alongside novel uses of blockchain and quantum computing, points to a future where cybersecurity is not just reactive, but predictive and adaptive. The drive towards global cooperation and stronger regulatory frameworks underscores the collective nature of this challenge. As the digital landscape continues to evolve, so too must the strategies employed to protect it, ensuring a dynamic and resilient defense against the ever-present threat of zero-day vulnerabilities.

2 Latest zero-day attacks

2.1 Microsoft Exchange Server Exploits (Hafnium Attack)

In early 2021, a state-sponsored group known as Hafnium exploited four zero-day vulnerabilities in Microsoft Exchange Server to access email accounts, install malware, and facilitate long-term access to victim networks. This case is notable for its impact on small and medium-sized businesses, government entities, and other organizations worldwide. The attackers used sophisticated techniques to bypass authentication, execute code on vulnerable servers, and create web shells for persistent access.

2.2 SolarWinds Supply Chain Attack

Although not a traditional zero-day exploit in the sense of exploiting previously unknown software vulnerabilities, the SolarWinds attack involved the compromise of the software development and distribution process to inject malicious code into a trusted software update. This campaign, identified towards the end of 2020, affected numerous government agencies and private organizations globally. The methodology used in this attack underscores the vulnerabilities in the software supply chain and the difficulty of detecting malicious activity within trusted systems.

2.3 Google Chrome V8 Zero-Day (CVE-2021-21224)

In April 2021, a zero-day vulnerability in the V8 JavaScript engine of the Google Chrome browser was exploited in the wild. This vulnerability allowed attackers to execute arbitrary code within the context of the browser, potentially leading to further system compromise if combined with other exploits. The exploit demonstrates the attractiveness of targeting widely used software like web browsers for zero-day attacks due to their extensive user base.

2.4 iOS Mail App Zero-Day (CVE-2020-9986)

Discovered being exploited in late 2020, this vulnerability in the Mail app on iOS devices allowed attackers to remotely infect devices by sending emails that consumed significant memory resources, leading to arbitrary code execution. This case highlights the challenges of securing mobile devices and the sophistication of attacks targeting them, often requiring no interaction from the victim.

2.5 Microsoft Exchange Server Exploits (Hafnium Attack)

Context: In March 2021, Microsoft reported that four zero-day vulnerabilities in its Exchange Server software were being exploited by Hafnium, a group assessed to be state-sponsored and operating out of China. The vulnerabilities allowed attackers to gain access to email accounts, install web shells for continued access, and deploy additional malware for long-term exploitation of the network.

Exploitation Techniques: The attackers used a multi-step process to exploit

these vulnerabilities. Initially, they would authenticate as the Exchange server. Then, they used the vulnerabilities to execute arbitrary code on the server, primarily to deploy web shells, enabling persistent access and control over the compromised environment.

Detection and Mitigation: Microsoft released emergency patches for the vulnerabilities and provided detailed guidance for detecting compromised systems. The scale of the attack led to a significant response from cybersecurity communities worldwide, including tools and scripts to automate the detection of compromises.

Implications: This incident highlighted the risks associated with complex software ecosystems and the importance of rapid patch management. It also underscored the need for improved security around authentication mechanisms and the potential for state-sponsored actors to target critical infrastructure.

2.6 SolarWinds Supply Chain Attack

Context: Discovered in December 2020, this sophisticated cyber espionage campaign compromised the software build system of SolarWinds, a company that produces network management software. The attackers inserted malicious code into the Orion software update, affecting thousands of organizations globally, including U.S. government agencies.

Exploitation Techniques: The attack was notable for its stealth and sophistication, using the trust relationship between software providers and their customers to distribute malware. The malicious code lay dormant for weeks or months, avoiding detection while collecting information and credentials.

Detection and Mitigation: The compromise was uncovered by a cybersecurity firm, which noticed suspicious activity within its own network. The detection highlighted the challenges in identifying supply chain compromises, leading to increased scrutiny of software development and distribution processes for security vulnerabilities.

Implications: The SolarWinds attack demonstrated the potential for supply chain attacks to have wide-reaching effects and the difficulty of defending against them. It has led to calls for more rigorous security practices in software development and greater cooperation between the public and private sectors in addressing cybersecurity threats.

2.7 Google Chrome V8 Zero-Day (CVE-2021-21224)

Context: In April 2021, Google reported a zero-day vulnerability in the V8 JavaScript engine of its Chrome browser, which was being actively exploited. The vulnerability could allow an attacker to execute arbitrary code within the Chrome browser by crafting malicious JavaScript content.

Exploitation Techniques: The exploit involved manipulating the memory

within the V8 engine using crafted JavaScript, leading to arbitrary code execution in the context of the browser. This could potentially lead to further system compromise if chained with other vulnerabilities.

Detection and Mitigation: Google addressed the vulnerability in an update to Chrome, urging users to update their browsers immediately. The quick response highlighted the importance of maintaining up-to-date software to mitigate the risks of zero-day exploits.

Implications: This case underscores the continuous arms race between software developers and attackers, emphasizing the need for robust browser security and the rapid patching of vulnerabilities as they are discovered.

2.8 iOS Mail App Zero-Day (CVE-2020-9986)

Context: Identified in late 2020, this vulnerability in the Mail app allowed attackers to remotely execute arbitrary code on iOS devices by sending specially crafted emails. The exploit did not require any interaction from the user, making it particularly insidious.

Exploitation Techniques: By sending an email that consumed a large amount of memory, attackers could trigger the vulnerability, leading to arbitrary code execution on the device. This could potentially compromise the device and allow for the extraction of sensitive information.

Detection and Mitigation: Apple released a patch for the vulnerability in a subsequent iOS update. The incident highlighted the importance of securing mobile email clients and the potential for zero-click exploits to bypass user interactions entirely.

Implications: The exploit demonstrated the evolving threat landscape for mobile devices and the need for ongoing vigilance and prompt updating of mobile operating systems to protect against emerging threats.

These case studies represent a cross-section of the zero-day exploit landscape, encompassing different targets, attackers, and impacts. The analysis will delve into the specifics of each exploit, examining the vulnerabilities involved, the attack methodologies, the identification and mitigation processes, and the broader implications for cybersecurity practices.

3 CHAPTER THREE TOPIC

CONCLUSION

Main results published in [1–4].

BIBLIOGRAPHY

1 Zero-Day Attack Detection and Prevention in Software-Defined Networks / Huthifh Al-Rushdan, M. Shurman, Sharhabeel H. Alnabelsi, Q. Althebyan // *2019 International Arab Conference on Information Technology (ACIT).* — 2019. — Pp. 278–282.

2 *Singh, Umesh Kumar.* A framework for zero-day vulnerabilities detection and prioritization / Umesh Kumar Singh, Chanchala Joshi, Dimitris Kanellopoulos // *Journal of Information Security and Applications.* — 2019. — Vol. 46. — Pp. 164–172.

3 The Effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers / Nikolaos Peppes, Theodoros Alexakis, Evgenia Adamopoulou, Konstantinos Demestichas // *Sensors.* — 2023. — Vol. 23, no. 2. — P. 900.

4 *Ye, Ziwei.* Zero-Day Vulnerability Risk Assessment and Attack Path Analysis Using Security Metric / Ziwei Ye, Yuanbo Guo, A. Ju. — 2019. — Pp. 266–278.

Appendix A Code listing

Simple code listing:

```
# Multiplication table (from 1 to 10) in Python

num = 12

# To take input from the user
# num = int(input("Display multiplication table of? "))

# Iterate 10 times from i = 1 to 10
for i in range(1, 11):
    print(num, 'x', i, '=', num*i)
```

Appendix B Second appendix

Some text

Appendix C Third appendix

Some text