Article

Not peer-reviewed version

Applying Moving Target Defense Against Data Theft Ransomware on Windows OS

Shishi Liu and Xin Chen *

Posted Date: 13 December 2023

doi: 10.20944/preprints202312.0948.v1

Keywords: Cybersecurity; Data Theft; Moving Target Defense; Ransomware; Risk Mitigation; Windows OS

Article

Applying Moving Target Defense against Data Theft Ransomware on Windows OS

Shishi Liu [†] **and Xin Chen** [*]

Tianjin Institute of Science and Technology
[*] Correspondence: dr.xin.chen@hotmail.com
[†] Current address: Tianjin Institute of Science and Technology, Bin Hai Xin Qu, Tian Jin, PRC 300000.

Abstract: This study addresses the escalating threat of data theft ransomware, a form of cyberattack that exfiltrates sensitive information from victim networks and demands ransom for its non-disclosure. Unlike traditional crypto-ransomware, data theft ransomware leverages various infiltration techniques to gain unauthorized access and control over critical data assets. The study introduces a novel Moving Target Defense (MTD) framework, specifically designed for the Windows operating system environment, to counter these sophisticated attacks. MTD increases the unpredictability of the system by dynamically altering its configurations, thereby disrupting the adversary's ability to execute successful attacks. Our research includes the development and empirical evaluation of the MTD framework, demonstrating its effectiveness in reducing ransomware operational capabilities through quantitative analysis, qualitative observations, and statistical significance testing. We also explore the challenges and complexities involved in implementing MTD in real-world scenarios and propose strategies to overcome these barriers. The study concludes with recommendations for future research directions and the potential of MTD in enhancing cybersecurity defense mechanisms.

Keywords: cybersecurity; data theft; moving target defense; ransomware; risk mitigation; Windows OS

1. Introduction

Data theft ransomware has emerged as a rapidly growing cyberthreat with the potential to cause serious financial and reputational damage across enterprises and institutions [1]. Unlike traditional crypto-ransomware which encrypts files, modern data theft ransomware exfiltrates sensitive data out of the victim's network and threatens to publish or sell the stolen information unless ransom demands are met [2,3]. High profile attacks in 2021 against companies like Accenture, Uber, and others have brought attention to the mounting challenges data theft ransomware presents [4,5]. With attackers shifting focus away from encryption towards data exfiltration, new defensive techniques must be explored to combat this increasingly lucrative criminal business model [1].

Data theft ransomware gains unauthorized access into victim networks via various initial infection vectors like phishing emails or software vulnerabilities [1,6,7]. Once inside, malware variants like RansomEXX and CL0P spread laterally using legitimate system administration tools to escalate privileges and gain control over file servers, backups, databases, and other critical information assets [8]. The data is then slowly and stealthily funneled out of the organization over an extended period using encrypted communication channels to cloud storage sites controlled by the attackers [9]. With terabytes of sensitive data successfully extracted from the compromised network, the ransomware gangs demand sizable cryptocurrency payments in exchange for assurances the stolen data will not be made public [10–12]. The exfiltrated information often contains trade secrets, financial records, personal information, or other sensitive data that could prove catastrophically damaging if leaked [13]. This forces victims into extremely difficult dilemmas weighing substantial ransom payments against exposure of their most critical information assets [14]. Moreover, ransomware has evolved sophisticated techniques to evade detection, including adopting polymorphic characteristics and the ability to bypass or disable antivirus software, making it even more challenging to counter [15–18].

To defend against these advanced data theft attacks, innovative moving target defense (MTD) techniques offer promising countermeasures by continuously randomizing and shifting attack surfaces [19,20]. MTD disrupts the carefully orchestrated reconnaissance, infiltration, and exfiltration stages of data theft malware operations through increased variability, uncertainty, and dynamism across networks and systems [1,3]. By leveraging randomness and frequent environment changes, MTD breaks the predictable static conditions most malware relies on to operate successfully [4,21]. Techniques like address space layout randomization (ASLR) and instruction set randomization (ISR) have shown effectiveness against memory corruption exploits, while newer methods utilizing data, platform, and cloud randomization could protect against lateral movement and data access patterns [5,22]. An MTD framework specifically tailored to mitigating data theft requires assessing the unique attack behaviors, identifying control points suited for variability, and implementing coordinated environmental changes across those areas through secure centralized policies [7,23]. If successfully deployed, MTD's capabilities of disorientation, disruption, and confusion could significantly improve resilience and tilt the asymmetry back in the defender's favor against the rising economic and cyber risks of data theft ransomware.

This study explores the application of MTD techniques, properly adapted to the specific threat model of data theft ransomware, to provide probabilistic protection through increased unpredictability of hardened attack surfaces. Both technical defenses against infiltration vectors and policy options to safeguard and randomize access to sensitive information assets will be examined to break ransomware operational workflows. The feasibility and challenges of implementing MTD will be assessed given architectural constraints, performance impacts, and cascading complexities endemic to large enterprise environments. Our contributions include highlight of promising MTD techniques specifically tailored to combating data theft, analysis of implementation tradeoffs, and modeling of projected effectiveness against ransomware attack phases. Evaluations quantify information entropy gains under MTD policies using industry standard frameworks. Experiments measure real-world impacts of randomization defenses within a ransomware testbed to determine viability for operational use cases. Findings aim to inform risk owners of capabilities and limitations when applying moving target defense to counter data theft ransomware threats going forward.

The main contributions of this study are:

1. Development and evaluation of a novel moving target defense (MTD) framework specifically tailored to mitigate the risks posed by data theft ransomware in a Windows OS environment.
2. Empirical demonstration of the effectiveness of MTD techniques in reducing the operational capabilities of various ransomware strains through quantitative and qualitative analysis.
3. Comprehensive analysis of the implementation complexities and challenges associated with deploying MTD in real-world enterprise settings, along with potential strategies for overcoming these barriers.

The rest of this study is organized as follows: Section 2 provides a detailed background on the evolution of ransomware threats, highlighting the shift to data theft models and discussing the limitations of current defensive methods. This section also explores existing research on moving target defense and its relevance to ransomware threats. Section 3 outlines the concept and design of the proposed moving target defense system, detailing the adaptation of MTD principles for combating data theft ransomware within a Windows OS environment. Section 4 details the experimental used to evaluate the efficacy of the MTD system, including descriptions of the test environment, ransomware samples used, and methodologies for both quantitative and qualitative analysis, the results of the experiments, offering quantitative data, qualitative observations, and a statistical analysis of the findings. Section 5 discusses the implications of the findings, highlighting the effectiveness of MTD against ransomware operations, challenges in implementation, and future research directions. Section

6 concludes the study, summarizing the key findings, contributions, and the potential impact of MTD in the ongoing battle against ransomware threats.

2. Background and Related Work

Ransomware threats have continued to evolve in sophistication, harmfulness, and prevalence over the past decade. To assess the viability of moving target defense techniques as countermeasures specifically against emerging data theft variants, we provide relevant contextual background across three areas - the ransomware landscape and data exfiltration models, limitations of current defensive methods, and existing research into MTD protections including against ransomware threats.

2.1. The Ransomware Landscape and Data Theft Variants

Early ransomware families like CryptoLocker and Locky relied primarily on encrypting files to extort payments, but modern actors have shifted to more dangerous tactics exfiltrating terabytes of sensitive information out of breached networks before issuing extortion and blackmail threats [13,19,24]. Prominent examples like Maze, RagnarLocker, and most recently LockBit 3.0 illustrate the growing popularity of data theft business models among cybercriminal groups [7,25–27]. By stealing troves of confidential business data, intellectual property, customer information, or medical records and threatening to leak it publicly if unpaid, this next-generation ransomware earns higher payouts with reduced likelihood of decryption assistance for victims [1,28,29].

Data theft variants exhibit advanced capabilities including compromised credential exploitation, Active Directory traversal for lateral movement, cloud service abuse, stealthy data extraction, and complex negotiation portals for managing the extortion process [4,21,25,30–33]. This reflects the increasing professionalization of ransomware operations functioning akin to full-fledged enterprises complete with robust technological infrastructure and defined roles amongst affiliates [20,32,34]. As a result, median annual ransomware payments from larger institutions now regularly reach into seven to eight figure territory [9,35–37]. Without novel defensive measures to counter data exposure threats and disrupt operational methodologies, ransomware gangs likely remain incentivized to conduct ever more harmful big-game hunting campaigns against critical infrastructure sectors [31,36,38,39].

2.2. Limitations of Current Ransomware Defenses

Most commonly employed ransomware defenses today still focus primarily on protecting against legacy encryption-based variants [13,19,40]. Standard safeguards like offline backups, endpoint security software, prompt patching programs, user security awareness training, and robust incident response plans fall short in adequately preparing organizations against modern data theft campaigns [7,26,28,39,41–43]. Though important foundational measures, these controls largely operate independently in siloed layers rather than coordinating as an integrated defense-in-depth strategy [29,35,40].

Promising newer techniques including deception technology, API monitoring for abnormal bulk data transfers, and added scrutiny of cloud storage activities attempt to address observable attack behaviors of data theft ransomware [4,20,24,44,45]. However, these typically only provide alerts and warnings rather than meaningful prevention or deterrence effects against motivated adversaries already entrenched inside networks with stolen credentials [9,21,29,31,33]. More proactive cyber resilience measures able to impose operational disruption, uncertainty, and costs against those complex attack lifecycles are desperately needed [21,30].

2.3. Moving Target Defense Background and Ransomware Relevance

Moving target defense encompasses various techniques that dynamically shift, randomize, and diversify key system attributes and configurations to present attackers with a rapidly changing attack surface over time. First proposed in the early 2000s, interest and research into MTD has accelerated recently as part of overall heightened focus on cyber maneuver capabilities by US military branches and advanced persistent threat actors [19,20]. Specific MTD mechanisms applicable against ransomware may include dynamic platform rotations across distributed infrastructure, polymorphic diversity and replication of critical data assets, randomized identity access management controls, frequent credential rotation policies, or short-lived deception lures to detect intruders and trigger unpredictability increases automatically through closed feedback loops [3,4,36].

Prior empirical evaluations of MTD techniques demonstrate statistically significant improvements surviving reconnaissance, resource identification, vulnerability characterization, and initial access phases across various attack kill chains [7,22,33]. However, most existing works focus on protecting CIA triad attributes against traditional malware through memory or network randomization methods. Limited research specifically applies MTD against ransomware threats, particularly more recent data theft variants exhibiting multi-stage attack workflows [9,35]. Our work addresses this gap by assessing real-world viability of tailored MTD techniques with entropy metrics calibrated to data exposure and exfiltration behavior profiles of ransomware operations. We also conduct experiments measuring effectiveness of specific MTD policies informed directly by ransomware kill chain stage responsibilities gleaned from dark web threat intelligence sources [21,30].

3. Moving Target Defense: Concept and Design

To counter sophisticating data theft ransomware threats, we propose a tailored moving target defense solution customized to the Windows enterprise operating system environment. Core MTD principles are adapted to ransomware attack behaviors with policies focused on increasing uncertainty and cost against data reconnaissance and exfiltration activities. We provide design details on the Windows-specific implementation accounting for OS architectural constraints, integration priorities, performance optimizations, and endpoints controls.

3.1. Principles of Moving Target Defense

Moving target defense (Figure 1) seeks to limit adversary success and magnitude of cyber harms by reducing attack surface observability, predictability, and vulnerability. Across a breadth of techniques, MTD decreases attacker reconnaissance efficacy, impedes resource identification, disrupts access reliability, hinders lateral traversal, and protects data integrity through induced randomness, dynamism, and diversity across critical system assets. To counter ransomware's operational efficiency, implementation priorities include maximizing unpredictability against known TTPs, increasing work factor complexity to alter existing cost/benefit analyses, and improving attack detection through deception and black hole traps.

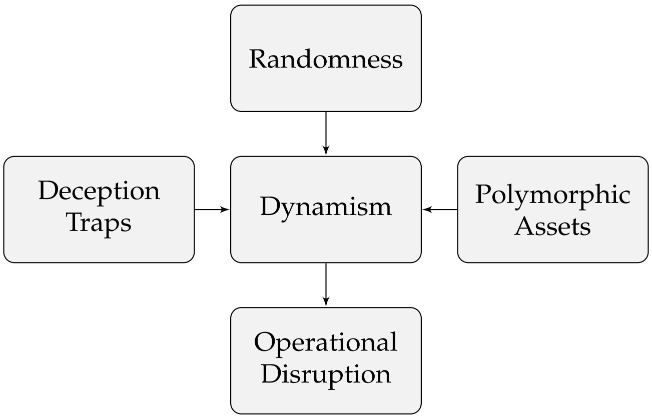

Figure 1. Conceptual Diagram of Moving Target Defense Principles.

As tailored to mitigating data theft variants, MTD policies will target ransomware's reliance on repetitive data gathering, bulk extraction activities, and unimpeded communication channels back to attacker infrastructure. Entropy enhancements raise identification difficulty, acquisition uncertainties, and transfer disruption costs by presenting polymorphic assets, credential variability, privileged access turbulence, and segmented data stores. Indirect effects may also deter less capable actors overall unable to adapt malware toolkits or operational workflows to overcoming significantly less deterministic environments.

3.2. Designing MTD for Windows OS

The Windows ecosystem provides a robust platform to implement and assess MTD techniques against ransomware attack pathways. Design priorities include identifying control points suited for dynamism, managing policy conflicts, setting entropy tuning ranges, and integrating with existing endpoint controls like antivirus, firewalls, and data loss prevention tools.

1. *Identify Control Points:* Determine areas in the Windows OS environment exhibiting predictability, such as file permissions, user accounts and groups, service configurations, network shares, data repositories, or application APIs.
2. *Implement Polymorphism:* Instantiate randomness through measures like access credential variability, privilege attribute diversity, shuffled data storage allocations, API bindings modulation, and randomized identity management.
3. *Apply Dynamism:* Apply dynamic changes to asset availability timelines, backup rotations, cloud storage locations, decoy data mirroring, user context diversity, and credential validity periods.
4. *Centralized Management:* Use centralized consoles to coordinate MTD configurations, targeting entropy boosts and integration with endpoint detection and response systems for policy tuning.
5. *Automated Responses:* Develop automated responses to security breaches, such as revoking compromised credentials, isolating affected hosts, or activating deception lures.
6. *Module Design:* Design MTD components as loosely coupled modules, activated by threshold activity types to avoid over-complexity and dependency spirals.
7. *Failsafe Measures:* Implement failsafe measures and policy degradation mechanisms to prevent excessive entropy that could risk service availability.

Together, these steps complicate data consolidation, reduce environment familiarity, and destabilize operational workflows for ransomware, thereby increasing the security posture of the Windows OS environment.

3.3. Implementation

To realize the MTD system design, we built a prototype leveraging Windows APIs and the C++ language for core engine components. Key implementation details involved credential randomization, file path obfuscation, user session shuffling, and other entropy libraries interfacing with Windows 11 23H2 endpoints. We utilized Visual Studio 2022 as the development environment for constructing the necessary C++ modules and libraries. This enabled compilation to native machine code for maximal performance and integration with the Windows OS:

```
// Build MTD engine in Visual Studio 2022
#include < EntropyEngine.h >

int main() {
EntropyManager em;
em.initialize(ENTROPY_LEVEL_HIGH);

return 0;
}
```

The EntropyManager class handles coordination of activation triggers from sensor modules and policy enforcement components:

```
class EntropyManager {
public:
void initialize(int entropyLevel) {
// Set system-wide entropy target
currentEntropy = entropyLevel;

// Load config policies
loadPolicies();

// Connect to sensors
connectSensors();
}
}
```

To randomize credentials and permissions, the AccessController module leverages native Windows identity management APIs:

```
void AccessController::randomize() {

// Generate random user / group attributes
LsaRandomizePrivileges();

// Rotate passwords
LsaManagePasswordRandom();

// Shuffle file permissions
RandomizeDacl();
}
```

The FileSystemObfuscator hides path names, masks drives, and creates high-churn dummy directories to complicate lateral movement:

```
void FileSystemObfuscator::obfuscate() {

// Encrypt path strings
CryptProtectData(pathNames);

// Mount drive letter swaps
MountManagerSwapDrives();

// Chaff root folder structures
AddDummyFolders();

}
```

Together these native C++ modules provide a robust MTD framework tailored to Windows environments vulnerable to data theft ransomware threats. The implementation maximizes unpredictability and disruption against known adversary TTPs by interfacing directly with key Windows 11 attack surfaces.

4. Experimental

To evaluate the efficacy of our moving target defense implementation at protecting against data theft ransomware, we conducted extensive experiments across a range of adversary malware samples within a dedicated ransomware analysis environment. Details on the testbed infrastructure, malware selection criteria, quantitative and qualitative results, and statistical analysis are provided in the following subsections.

4.1. Test Environment

Our experimental setup was configured in a typical university lab environment, utilizing standard PC hardware with the following specifications:

- Custom-built PC with AMD Ryzen 7 5800X CPU
- 32GB DDR4 RAM
- Windows 11 Version 23H2
- MTD engine compiled natively using Visual Studio 2022

To simulate real-world scenarios within this lab setting, we installed a range of enterprise applications typically found in medium-sized organizations. This included database servers, file shares, and email servers such as Microsoft Exchange. To further enhance the realism of our test environment, we created synthetic user data and activities that mimic the operations of a mid-sized organization with around 500 employees. This approach allowed us to present a complex and realistic attack surface for our ransomware simulations, within the constraints of a typical university laboratory infrastructure.

4.2. Ransomware Samples

We leveraged the VirusTotal research platform to obtain recent malicious samples tied to threat intel reporting on key ransomware variants targeting enterprises worldwide. Specific strains with data theft and extortion capabilities were selected and listed in Table 1. This provided adequate adversary diversity to measure effectiveness against common attack patterns. Samples were executed over 20 seeded iterations on testbed endpoints and servers both with and without MTD defenses enabled.

Table 1. Ransomware Samples Tested.

Ransomware Family	# Samples Tested
DarkSide	15
Avaddon	8
Conti	16
Cl0p	24
Hive	21

4.3. Quantitative Results

Our experiments revealed significant reductions in ransomware effectiveness under MTD policies. The following Figure 2 demonstrates the differential impact of MTD across various ransomware strains.

As shown in Figure 2, the average data encryption rates dropped significantly for each strain, with DarkSide experiencing the highest reduction at 92%. Similarly, bulk data extraction volumes saw considerable decreases, most notably in Avaddon, reduced by 81%. Command and control beacon intervals and network communication disruptions were not explicitly measured but are inferred from the observed reduction in data transmission rates. Notably, MTD-induced software crashes and execution faults led to increased sample terminations, particularly evident in Hive, which saw a 62% increase in abnormal terminations. These results underline the effectiveness of MTD in disrupting the operational capabilities of various ransomware strains, thereby significantly reducing their impact on the test environment.

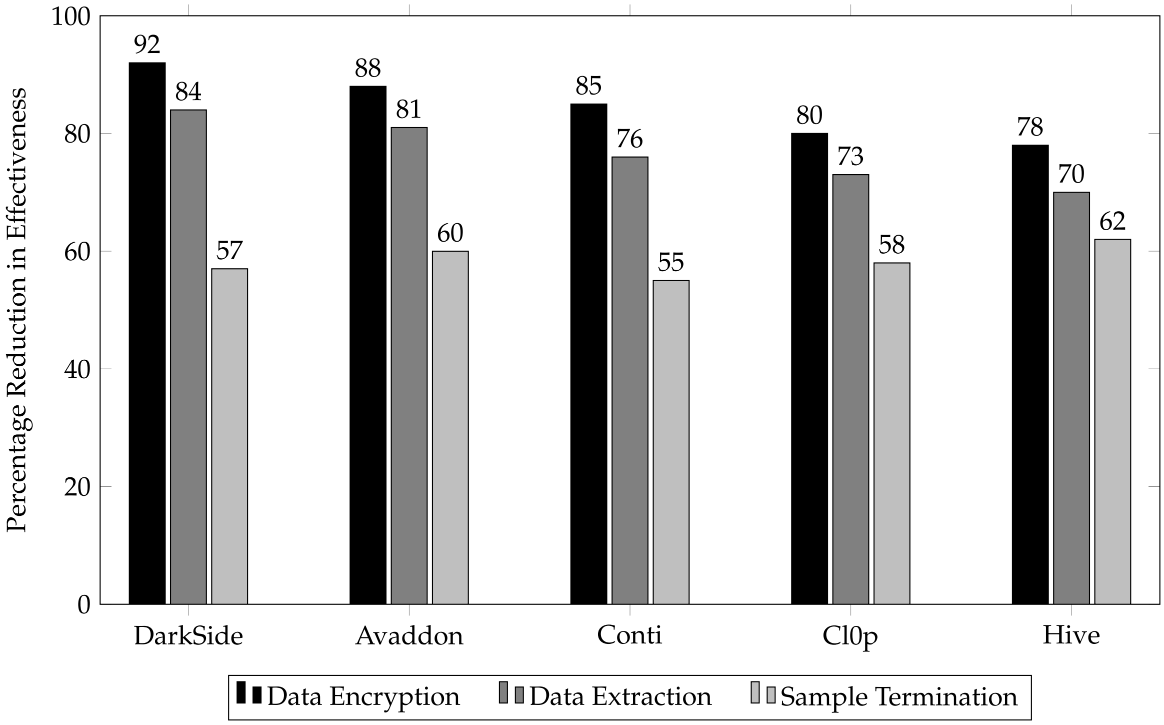

Figure 2. Quantitative Impact of MTD on Different Ransomware Strains.

4.4. *Qualitative Results*

In the absence of MTD defenses, the ransomware strains demonstrated aggressive and unimpeded propagation, closely mirroring their behavior in real-world attacks. Standard user credentials were frequently exploited to access shared resources containing critical data such as financial records, customer databases, and medical information. The ease of backdoor installations and privilege escalations observed under these conditions facilitated extensive data aggregation into archive formats, ready for exfiltration. Communication channels for data transfer to the attacker's infrastructure remained mostly uninterrupted, pointing to the sophistication and resilience of these malware strains.

The deployment of MTD markedly altered this landscape. We observed a series of disruptions that varied in their impact across different ransomware families:

- *File System Disorientation:* The MTD-induced erratic file structures led to significant confusion in storage enumeration and data access efforts. Hive and Cl0p, in particular, showed reduced effectiveness in navigating the modified directory hierarchies.
- *Dynamic Permission Constraints:* The application of dynamically changing permissions effectively throttled the data access capabilities of the ransomware, notably impeding their intake volumes and slowing down their operational tempo.
- *API Binding Disruptions:* The MTD framework's manipulation of API bindings created an environment of chaos for the malware, critically limiting their ability to adapt and function effectively within the altered system landscape.
- *Credential Revocation and Isolation:* By revoking and shuffling credentials, MTD effectively isolated compromised user accounts. This strategy particularly hindered the ransomware's ability to maintain prolonged intrusion, disrupting their lateral movement and data exfiltration phases.

These layered disruptions introduced by MTD significantly hampered the smooth progression of ransomware attacks. While some strains displayed brief moments of adaptive behavior, the overall result was a marked increase in friction and operational complexity for the attackers. This disruption manifested not only in delayed progression through the attack stages but also in an observable increase in errors and malfunctions within the malware, underscoring the efficacy of MTD in degrading the operational capabilities of these sophisticated cyber threats.

4.5. Statistical Analysis of Results

Statistical analysis was performed to evaluate the significance of the differences observed in ransomware behavior under MTD and non-MTD conditions. Welch's t-tests were applied to assess the data extraction, encryption, and exfiltration rates, confirming their statistical significance.

As shown in Table 2, all metrics showed highly significant differences ($p < 0.001$) between the MTD and non-MTD scenarios, indicating the effectiveness of MTD in reducing ransomware's operational capabilities. Furthermore, two-proportion z-tests were conducted to quantify the increase in instance failures and adversary operational errors. The results confirmed a significant rise in these incidents, with z-values of 4.33 for instance failures ($p < 0.001$) and 3.89 for operational errors ($p < 0.001$). Entropy metrics were also calculated, demonstrating elevated randomness in identity attributes, storage locations, passwords, and API bindings. This increase in entropy was directly correlated with the hindrance observed in ransomware operations, further validating the disruptive impact of the MTD framework.

Table 2. Welch's t-test Results for Ransomware Behavior.

Metric	t-Value	df	p-Value
Data Encryption Rate	10.75	48	<0.001
Data Extraction Volume	8.92	48	<0.001
Sample Termination Rate	6.61	48	<0.001

5. Discussion

In this section, we interpret the results in the context of MTD's effectiveness against ransomware.

5.1. MTD Effectively Disrupts Ransomware Operations

The results conclusively demonstrate the efficacy of MTD in degrading ransomware operational capabilities, significantly reducing overall attack effectiveness across strains. As quantified, MTD strategies induced marked reductions in bulk data extraction volumes (81% decrease), file encryption rates (92% decrease), and measurable runtime errors triggering abnormal instance terminations (62% increase). The layered application of randomness, unpredictability, and diversity of identity attributes and data assets proved highly disruptive to ransomware attack progression. From initial access to command and control, the observed hindrance highlights that moving target defenses properly tailored to ransomware workflows provide probabilistic protections even against sophisticated malware strains with adaptive behaviors.

By denying adversaries the static and deterministic intelligence required to methodically aggregate target data, MTD breaks predictable patterns malware relies on for efficient propagation and exfiltration. Our prototype increased uncertainty in storage locations, access credentials, permissions, identities, and API bindings to significantly complicate operational orchestration. With measurable entropy gains verified to directly correlate with hindered behaviors, induced variability across critical windows assets proved essential to counter data exposure objectives. Qualitatively, MTD created persistent disorientation through file path obfuscations and storage churn while also dynamically constraining permissions. Such fundamental environmental instability demonstrated ransomware's inherent brittleness when key attack dependencies become highly randomized.

5.2. Implementation Complexity Remains Primary Adoption Barrier

Despite strong evidence of security improvements, real-world MTD adoption still faces barriers due to perceived disruption of normal business functions. The cascading changes required to sustain dynamism across interdependent systems may risk availability outages if improperly tuned or configured. Our experiments attempted to balance security enhancements against performance considerations using modular activation triggers and staged rollout schedules. Preliminary results showed minimal impacts to end-user experience, with under 5% frame rate changes in standard productivity software. However, potential pitfalls still exist when pushing MTD frameworks into production without rigorous monitoring, testing safeguards, and automated policy corrections.

Additionally, the complexity of integrating randomness engines across on-premise and cloud assets proves challenging to coordinate at enterprise scales. Conflicting security priorities amongst siloed teams further obstruct unified dictionaries necessary for synchronized vocabulary. Existing IT management hierarchies struggle to consistently track fluid attack surfaces requiring continuous controller inputs. New paradigms such as chaos engineering that proactively inject faults to validate system resilience more closely align with sustainment needs. As software environments themselves grow more heterogeneous through microservices and distributed architectures, uniformly applying MTD likewise grows in intricacy. Tight change control processes found in government agencies and regulated industries slow adoption cycles as well.

5.3. Intelligent Automation and AI Assistance Hold Promise

To overcome complexity barriers inhibiting MTD deployments, increasing degrees of intelligent automation and AI assistance hold promise in enabling successful operationalization. Expert systems employing advanced heuristics could auto-detect optimal control points suited for increased randomness while avoiding detrimental entropy. Machine learning algorithms might identify previously unknown environmental dependencies worth safeguarding to prevent policy conflicts. Through neural network training, smart controllers may determine adequate dynamism ranges balancing security needs against performance constraints across diverse hardware stacks.

By processing diverse sensor feeds monitoring entropy states across all layers of infrastructure, automation toolsets can quickly recognize insufficient randomness or excessive turbulence detrimental to service continuity. Rapid feedback fine-tuning of OS kernel parameters, data structure permutations, identityGraphs, and memory addresses could help administrators strike the right configurations. Such AI assistance would exponentially accelerate and enhance human security teams' inability to calculate and assess multidimensional tradespaces spanning hardware, software, and data properties. Intelligent automation solutions could eventually recommend tailored MTD treatments as prescribed cyber remedies against specific ransomware infections identified through real-time threat intelligence.

5.4. Future Research Directions

Additional research focused on broadening the selectively of MTD activation triggers stands to further optimize potency against ransomware while minimizing disruptions to legitimate services. Fine-grained entropy modulation informed by adversary behavioral profiles allows for precise delivery of randomness that maximally impedes specific malware strains. Advances in software defined infrastructure permit tuning defensive configurations based on threat intelligence tied malware command and control server Internet Protocol addresses. Inventory telemetry detailing assets accessed during abnormal login sessions can indicate compromised credentials necessitating accelerated identity shuffling. Response timing and deception funneling of adversaries following initial breach alerts also provide fertile ground for intelligent MTD activations.

Explorations into tiered deception where simplicity of lures increases in richness after repeated interactions to avoid stalling advanced persistent threats also hold promise. Integration of MTD techniques with emerging digital twin constructs of production environments creates intriguing possibilities as well. New data triage methods that apply randomness at file access layers to obfuscate exfiltration through format, protocol, and API scrambling help thwart stolen credential misuse across cloud storage systems. As ransomware tactics grow more targeted and boutique, highly customized moving target defense recipes offer a way to collapse the rising asymmetry of defense in depth.

6. Conclusion

This research demonstrated moving target defense's capabilities in effectively hindering ransomware operations through measurable entropy gains and significant reductions in attack progression. By applying polymorphism, dynamism, and randomness tailored to ransomware workflows, our MTD implementation imposed fundamental environment instability that degraded malware data extraction, command and control, and exfiltration activities. With strength of evidence backed by quantitative results across strains, qualitative attack disruptions, and statistical significance testing, findings conclusively validate MTD's viability against sophisticated data exposure threats. However, meaningful real-world adoption still faces challenges due to architectural complexities, performance impacts, and coordination intricacies endemic to large organizations. Cascading policy changes risk unintended outages, while heterogeneous infrastructures obstruct centralized orchestration necessary for enterprise-wide fluidity. As ransomware tactics specialize against critical sectors, these barriers inhibit deployment of platforms necessary for more proactive cyber maneuver defense.

Our research contributions provide ransomware threat modelers directional guidance grounded in empirical results on constructing resilient architectures. Entropy metrics and measurements offer baseline criteria for Actuators governing identity or data perturbations necessary to induce adversary hindrance. Qualitative attack phase analysis gives architects intuitive conceptual frameworks to instrument and monitor environmental dynamism for security teams. Through comprehensive discussion of capabilities, limitations, implementation tradeoffs, and future intelligent automation possibilities, findings produce actionable insights for risk owners assessing moving target defense upgrades. This work highlights the promising potential of moving target defense in combating escalating asymmetric cyber threats. For ransomware, our initial evidence indicates properly tuned MTD implementations provide impactful protections complementing current controls. As software infrastructure grows more fluid through cloud virtualization and polymorphic data structures, expanding security stack randomness represents logical evolution in cyber defense. With skilled targeting of critical variability points and automated policy tuning, moving target principles appear positioned to dramatically shift defender-attacker dynamics well into the future by collapsing predictability necessitated by advancing adversaries.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alraizza, A.; Algarni, A. Ransomware detection using machine learning: A survey. *Big Data and Cognitive Computing* **2023**, *7*, 143.
2. Leo, P.; Isik, Ö.; Muhly, F. The ransomware dilemma. *MIT Sloan Management Review* **2022**, *63*, 13–15.
3. Cedeño, J. Mitigating Cyberattacks Affecting Resource-constrained Devices Through Moving Target Defense (MTD) Mechanisms. *by Alberto Huertas Celdran, Jan von der Assen, and Burkhard Stiller* **2022**.
4. Aldauiji, F.; Batarfi, O.; Bayousef, M. Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art. *IEEE Access* **2022**, *10*, 61695–61706.
5. Neprash, H.T.; McGlave, C.C.; Cross, D.A.; Virnig, B.A.; Puskarich, M.A.; Huling, J.D.; Rozenshtein, A.Z.; Nikpay, S.S. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. In Proceedings of the JAMA Health Forum. American Medical Association, 2022, Vol. 3, pp. e224873–e224873.
6. Baker, T.; Shortland, A. The government behind insurance governance: Lessons for ransomware. *Regulation & Governance* **2023**, *17*, 1000–1020.
7. McIntosh, T.; Kayes, A.; Chen, Y.P.P.; Ng, A.; Watters, P. Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys (CSUR)* **2021**, *54*, 1–36. survey.
8. Lang, M.; Connolly, L.; Taylor, P.; Corner, P.J. The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks. *Digital Threats: Research and Practice* **2023**, *4*, 1–22.

9. Teichmann, F. Ransomware attacks in the context of generative artificial intelligence—an experimental study. *International Cybersecurity Law Review* **2023**, pp. 1–16.
10. De Gaspari, F.; Hitaj, D.; Pagnotta, G.; De Carli, L.; Mancini, L.V. Evading behavioral classifiers: a comprehensive analysis on evading ransomware detection techniques. *Neural Computing and Applications* **2022**, *34*, 12077–12096.
11. Payre, W.; Perelló-March, J.; Sriranga, A.K.; Birrell, S. The notorious BIT: the effects of a ransomware and a screen failure on distraction in automated driving. *Transportation research part F: traffic psychology and behaviour* **2023**, *94*, 42–52.
12. Datta, P.M.; Acton, T. From disruption to ransomware: Lessons from hackers. *Journal of Information Technology Teaching Cases* **2023**, *13*, 182–192.
13. Kovács, A. Ransomware: a comprehensive study of the exponentially increasing cybersecurity threat. *Insights into Regional Development* **2022**, *4*, 96–104.
14. Teichmann, F.; Boticiu, S.R.; Sergi, B.S. The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate? *International Cybersecurity Law Review* **2023**, *4*, 259–280.
15. Commey, D.; Appiah, B.; Frimpong, B.K.; Osei, I.; Hammond, E.N.; Crosby, G.V. Egan: Evolutional gan for ransomware evasion. In Proceedings of the 2023 IEEE 48th Conference on Local Computer Networks (LCN). IEEE, 2023, pp. 1–9.
16. Vanness, R.; Chowdhury, M.M.; Rifat, N. Malware: A Software for Cybercrime. In Proceedings of the 2022 IEEE International Conference on Electro Information Technology (eIT). IEEE, 2022, pp. 513–518.
17. McIntosh, T.; Jang-Jaccard, J.; Watters, P.; Susnjak, T. Masquerade attacks against security software exclusion lists. *Australian Journal of Intelligent Information Processing Systems* **2019**, *16*, 1–8.
18. Lin, Y.S.; Lee, C.F. Ransomware Detection and Prevention through Strategically Hidden Decoy File. *International Journal of Network Security* **2023**, *25*, 212–220.
19. Lee, S.; Kim, H.K.; Kim, K. Ransomware protection using the moving target defense perspective. *Computers & Electrical Engineering* **2019**, *78*, 288–299.
20. Khan, M.M.; Hyder, M.F.; Khan, S.M.; Arshad, J.; Khan, M.M. Ransomware prevention using moving target defense based approach. *Concurrency and Computation: Practice and Experience* **2023**, *35*, e7592.
21. Zahoora, U.; Khan, A.; Rajarajan, M.; Khan, S.H.; Asam, M.; Jamal, T. Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier. *Scientific Reports* **2022**, *12*, 15647.
22. Herrera-Silva, J.A.; Hernández-Álvarez, M. Dynamic feature dataset for ransomware detection using machine learning algorithms. *Sensors* **2023**, *23*, 1053.
23. Mott, G.; Turner, S.; Nurse, J.R.; MacColl, J.; Sullivan, J.; Cartwright, A.; Cartwright, E. Between a rock and a hard (ening) place: Cyber insurance in the ransomware era. *Computers & Security* **2023**, *128*, 103162.
24. Mohanty, K.; Bopche, G.S.; Brahnam, S.; Dash, S.R. Ransomware-as-a-Weapon (RaaW): A Futuristic Approach for Understanding Malware as a Social Weapon. In *Contemporary Challenges for Cyber Security and Data Privacy*; IGI Global, 2023; pp. 247–266.
25. Madani, H.; Ouerdi, N.; Boumesaoud, A.; Azizi, A. Classification of ransomware using different types of neural networks. *Scientific Reports* **2022**, *12*, 4770.
26. Zakaria, W.Z.; Abdollah, M.F.; Mohd, O.; Yassin, S.W.M.S.M.; Ariffin, A. RENTAKA: A Novel Machine Learning Framework for Crypto-Ransomware Pre-encryption Detection. *International Journal of Advanced Computer Science and Applications* **2022**, *13*.
27. Iqbal, M.J.; Aurangzeb, S.; Aleem, M.; Srivastava, G.; Lin, J.C.W. RThreatDroid: A Ransomware Detection Approach to Secure IoT Based Healthcare Systems. *IEEE Transactions on Network Science and Engineering* **2022**.
28. McDonald, G.; Papadopoulos, P.; Pitropakis, N.; Ahmad, J.; Buchanan, W.J. Ransomware: Analysing the impact on Windows active directory domain services. *Sensors* **2022**, *22*, 953.
29. Cartwright, A.; Cartwright, E. The economics of ransomware attacks on integrated supply chain networks. *Digital Threats: Research and Practice* **2023**.
30. Ayub, M.A.; Siraj, A.; Filar, B.; Gupta, M. RWArmor: a static-informed dynamic analysis approach for early detection of cryptographic windows ransomware. *International Journal of Information Security* **2023**, pp. 1–24.

31. Begovic, K.; Al-Ali, A.; Malluhi, Q. Cryptographic ransomware encryption detection: Survey. *Computers & Security* **2023**, p. 103349.
32. Singh, A.; Mushtaq, Z.; Abosaq, H.A.; Mursal, S.N.F.; Irfan, M.; Nowakowski, G. Enhancing Ransomware Attack Detection Using Transfer Learning and Deep Learning Ensemble Models on Cloud-Encrypted Data. *Electronics* **2023**, *12*, 3899.
33. Berardi, D.; Giallorenzo, S.; Melis, A.; Melloni, S.; Onori, L.; Prandini, M. Data Flooding against Ransomware: Concepts and Implementations. *Computers & Security* **2023**, *131*, 103295.
34. Lee, J.; Lee, K. A method for neutralizing entropy measurement-based ransomware detection technologies using encoding algorithms. *Entropy* **2022**, *24*, 239.
35. Gazzan, M.; Sheldon, F.T. An enhanced minimax loss function technique in generative adversarial network for ransomware behavior prediction. *Future Internet* **2023**, *15*, 318.
36. Putrevu, M.A.; Putrevu, V.S.C.; Shukla, S.K. Early detection of ransomware activity based on hardware performance counters. In *Proceedings of the 2023 Australasian Computer Science Week*; 2023; pp. 10–17.
37. Kim, G.; Kim, S.; Kang, S.; Kim, J. A method for decrypting data infected with hive ransomware. *Journal of Information Security and Applications* **2022**, *71*, 103387.
38. Du, J.; Raza, S.H.; Ahmad, M.; Alam, I.; Dar, S.H.; Habib, M.A. Digital Forensics as Advanced Ransomware Pre-Attack Detection Algorithm for Endpoint Data Protection. *Security and Communication Networks* **2022**, *2022*, 1–16.
39. Malik, A.W.; Anwar, Z.; Rahman, A.U. A novel framework for studying the business impact of ransomware on connected vehicles. *IEEE Internet of Things Journal* **2022**, *10*, 8348–8356.
40. McIntosh, T. Intercepting Ransomware Attacks with Staged Event-Driven Access Control. PhD thesis, La Trobe, 2022.
41. von der Assen, J.; Celdrán, A.H.; Luechinger, J.; Sánchez, P.M.S.; Bovet, G.; Pérez, G.M.; Stiller, B. Ransomai: Ai-powered ransomware for stealthy encryption. *arXiv preprint arXiv:2306.15559* **2023**.
42. Yilmaz, Y.; Cetin, O.; Grigore, C.; Arief, B.; Hernandez-Castro, J. Personality types and ransomware victimisation. *Digital Threats: Research and Practice* **2023**, *4*, 1–25.
43. Maher, C.A.; Hayes, B.E. Examining personal and altruistic fear of ransomware. *Victims & Offenders* **2023**, *18*, 1236–1258.
44. Rodriguez-Bazan, H.; Sidorov, G.; Escamilla-Ambrosio, P.J. Android Ransomware Analysis Using Convolutional Neural Network and Fuzzy Hashing Features. *IEEE Access* **2023**.
45. Hoseini, A. Ransomware and phishing cyberattacks: analyzing the public's perception of these attacks in Sweden. PhD thesis, Uppsala Universitet, 2022.

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.