TRILLIUM
INFORMATION SECURITY SYSTEMS

DFIR

INSIGHTS REPORT

2023

TISS
CYBERSECURITY
INSIGHTS

TABLE OF CONTENTS

INTRODUCTION

In today's rapidly evolving digital landscape, the idea of achieving complete protection from cyber attacks is a myth. Cyber threats are now an inevitability, making it not a matter of if an attack will occur, but when. Given this certainty, the ability to respond immediately and effectively is crucial. This is where Digital Forensics and Incident Response (DFIR) becomes essential.

Over the past year, our DFIR team has led numerous cyber engagements, uncovering crucial insights from a variety of incidents. This report distills our comprehensive findings, highlighting the most targeted sectors, the common types of attacks, the most notorious ransomware groups, and the advanced tactics used by attackers. Additionally, we outline the critical controls that could have mitigated these threats.

By sharing our expertise, we aim to empower cybersecurity practitioners with the knowledge and tools needed to navigate and combat cyber threats in today's dynamic and challenging digital environment. This means providing insights into emerging threats, best practices for incident response, and practical advice for implementing effective security measures. Our goal is to strengthen collective resilience, ensuring that individuals and organizations are better equipped to defend against cyber attacks. By improving defenses and fostering a culture of cybersecurity awareness, we can reduce the likelihood and impact of cyber incidents, ultimately creating a safer digital ecosystem for all.

KEY TAKEAWAYS FROM THE REPORT

TOP TARGETED SECTORS

Government
Financial
IT & Telecom

TOP ATTACKS IDENTIFIED

Ransomware
Data Breach
Injection Attacks

TOP RANSOMWARE GROUPS

BlackCat (AlphaV)
LockBit
Medusa

TOP SECURITY CONTROLS

Endpoint Detection and Response
Dedicated SOC
User Awareness
Privileged Access Management

TOP USED TACTICS

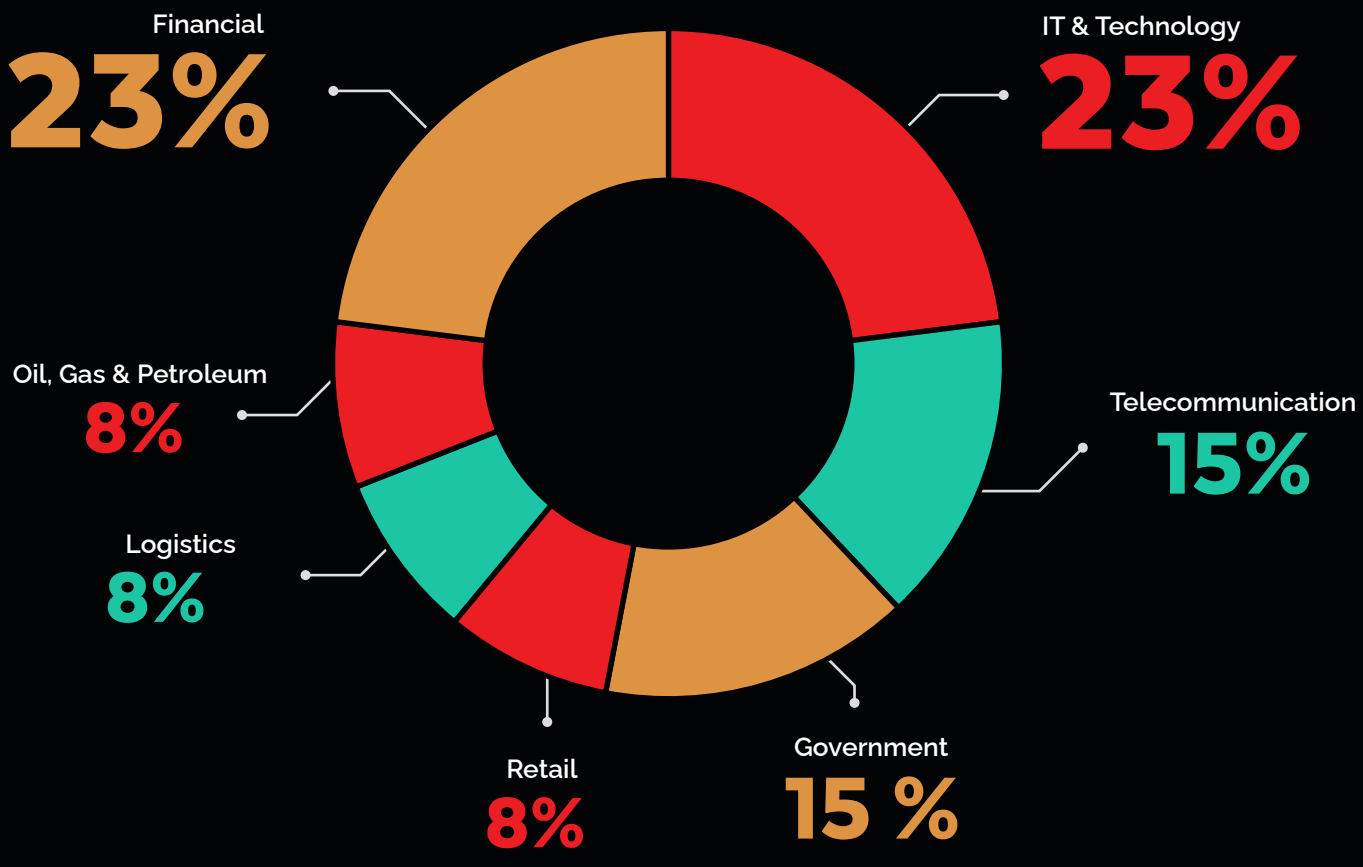
Execution
Persistence
Defense Evasion

ENGAGEMENT OVERVIEW

In 2023, leading organizations across various industries in Pakistan experienced significant cyberattacks, showcasing the pervasive threat posed by cybercriminals. Trillium Information Security Systems (TISS) played an instrumental role in mitigating these attacks by offering specialized Digital Forensics and Incident Response (DFIR) services to key industrial organizations, government bodies, and critical infrastructure providers nationwide. TISS's swift and proactive response was particularly impactful in the IT & Technology and Financial sectors, which together accounted for the highest number of attacks, each representing 23% of the total incidents. Our expert interventions helped these organizations recover quickly and bolster their defenses against future threats.

MAJOR CYBERATTACK TARGETS IN PAKISTAN [2023]

As cyberattacks become more sophisticated, building resilience and adopting proactive defense strategies have become essential for organizations to withstand and prevent future attacks. The following data highlights the industries most affected by cyberattacks over the past year. The IT & Technology and Financial sectors emerged as the top targets, each experiencing 23% of the total attacks, followed by the Telecommunication and Government sectors, each at 15%. Other sectors impacted include Retail, Logistics, and Oil, Gas & Petroleum, each accounting for 8% of the total incidents.

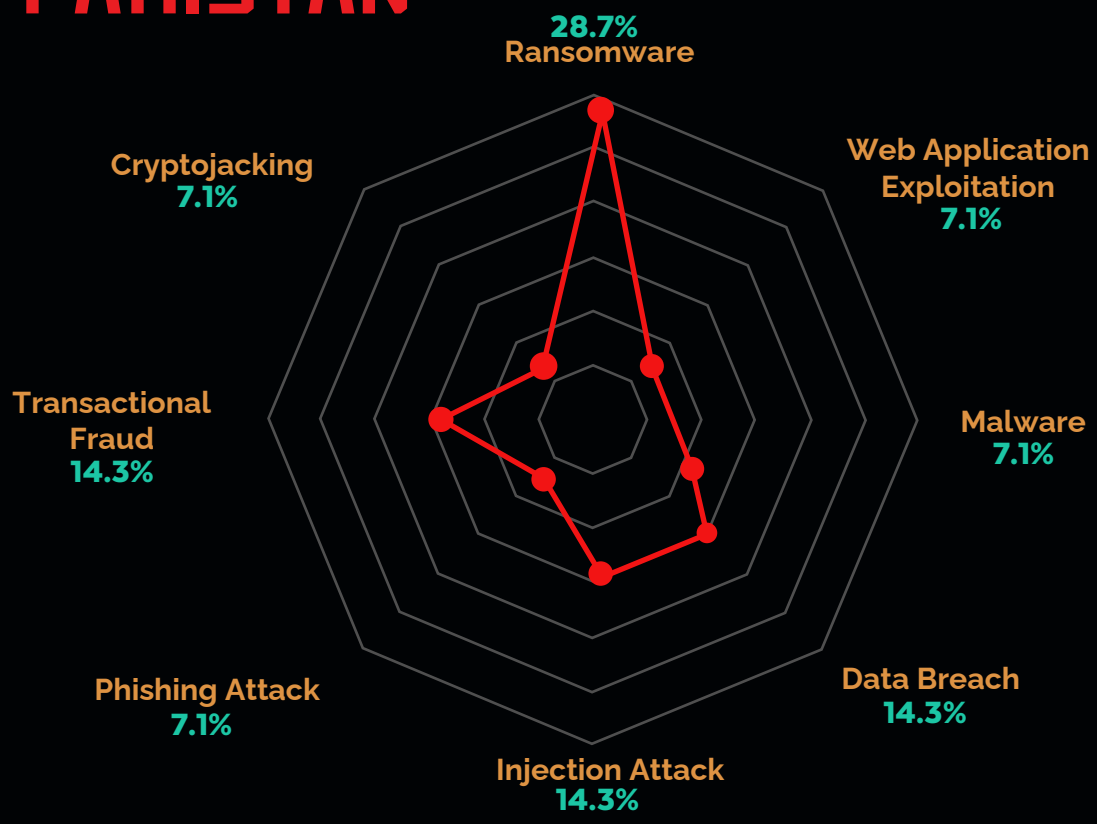


KEY CYBER THREATS TACKLED BY TISS

TISS has been at the forefront of providing cybersecurity services to government and private organizations in Pakistan, addressing a diverse range of cyberattacks. In 2023, ransomware attacks were particularly prominent, accounting for 28.7% of the incidents we managed. Data breaches and injection attacks each represented 14.3% of the incidents handled during this period. Additionally, transactional frauds and web application exploitation each made up 14.3% of the attacks addressed. Phishing attacks, cryptojacking, and malware incidents, though less frequent, still presented significant threats and contributed to disruptions in business operations.

Ransomware groups have been notably active, targeting major financial and industrial organizations and causing substantial damage to critical data. Injection attacks have led to significant reputational harm for various organizations. Phishing attacks, cryptojacking, and malware have also caused considerable disruptions. The exploitation of mobile banking applications has resulted in considerable financial losses through transactional fraud. Overall, the financial repercussions of these attacks are substantial, often involving hefty ransom payments and prolonged downtime, which disrupts business operations and erodes trust.

SIGNIFICANT CYBERATTACKS IN PAKISTAN



MAIN CAUSES OF ATTACKS

Did you know why many cyberattacks have been successful in recent years? It's often due to the non-implementation or misconfiguration of crucial security controls such as Endpoint Detection and Response (EDR), user awareness programs, a dedicated Security Operations Center (SOC) team, and effective patch management. When these controls are properly implemented, they can significantly reduce the risk of successful cyberattacks.

Let's explore each of these security controls and their importance:

EDR (ENDPOINT DETECTION AND RESPONSE)

Importance: Provides real-time endpoint monitoring through telemetry
Implementation Benefits: Swift detection and containment of advanced threats

DEDICATED SOC TEAM

Importance: Provides continuous security monitoring.
Implementation Benefits: Timely incident response, threat intelligence utilization.

EPP (ENDPOINT PROTECTION PLATFORM) MISCONFIGURATIONS

Importance: Ensures endpoint protection from malware, exploits, host intrusion prevention, and some advanced persistent threats (APTs).
Implementation Benefits: Proper configuration enhances threat detection and endpoint visibility, reducing exposure to undetected attacks.

PAM (PRIVILEGED ACCESS MANAGEMENT) ABSENCE

Importance: Controls and monitors privileged access to critical systems, preventing unauthorized access and privilege **escalation.**
Implementation Benefits: Limits unauthorized access, privilege escalation, and lateral movement, securing critical data and systems.

USER AWARENESS TRAINING

Importance: Strengthening human firewalls
Implementation Benefits: Empowered users reduced social engineering risks.

TIMELY PATCH MANAGEMENT

Importance: Vulnerability mitigation.
Implementation Benefits: Reduced attack surface, enhanced system security

THREAT PYRAMID

The Threat Pyramid categorizes cyber threats based on their sophistication and impact, offering insights into the evolving nature of cybersecurity challenges. It is based on three main categories:

Advanced Persistent Threats (APTs)

These are highly sophisticated, persistent attacks orchestrated by well-funded adversaries. APTs aim for long-term access to sensitive information.

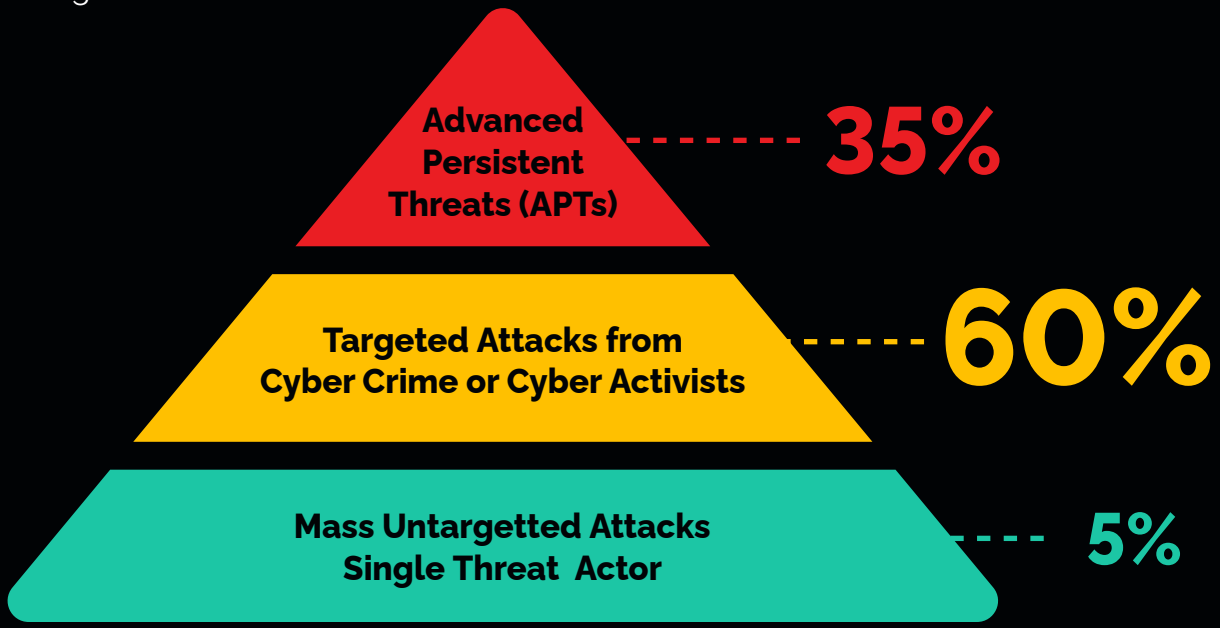
Targeted Attacks

These are precision-focused campaigns tailored to specific high-value targets. They often leverage advanced tactics like social engineering and insider knowledge.

Mass Attacks

These are widespread attacks, often exploiting known vulnerabilities. They are typically carried out through methods like phishing and malware distribution.

Among the attacks investigated by Trillium Information Security Systems (TISS), 35% of attacks were associated with APTs, 60% were Targeted Attacks on organizations, and 5% were Mass Untargeted Attacks.



IMPLICATIONS FOR CYBERSECURITY

Organizations must prioritize vigorous security investments and proactive defenses to mitigate risks from advanced adversaries. Understanding the threat distribution in the Threat Pyramid enables effective resource allocation and strategy implementation across the spectrum of cyber threats. This proactive approach enhances threat detection and response, reducing the likelihood of successful attacks while safeguarding sensitive information and ensuring business continuity

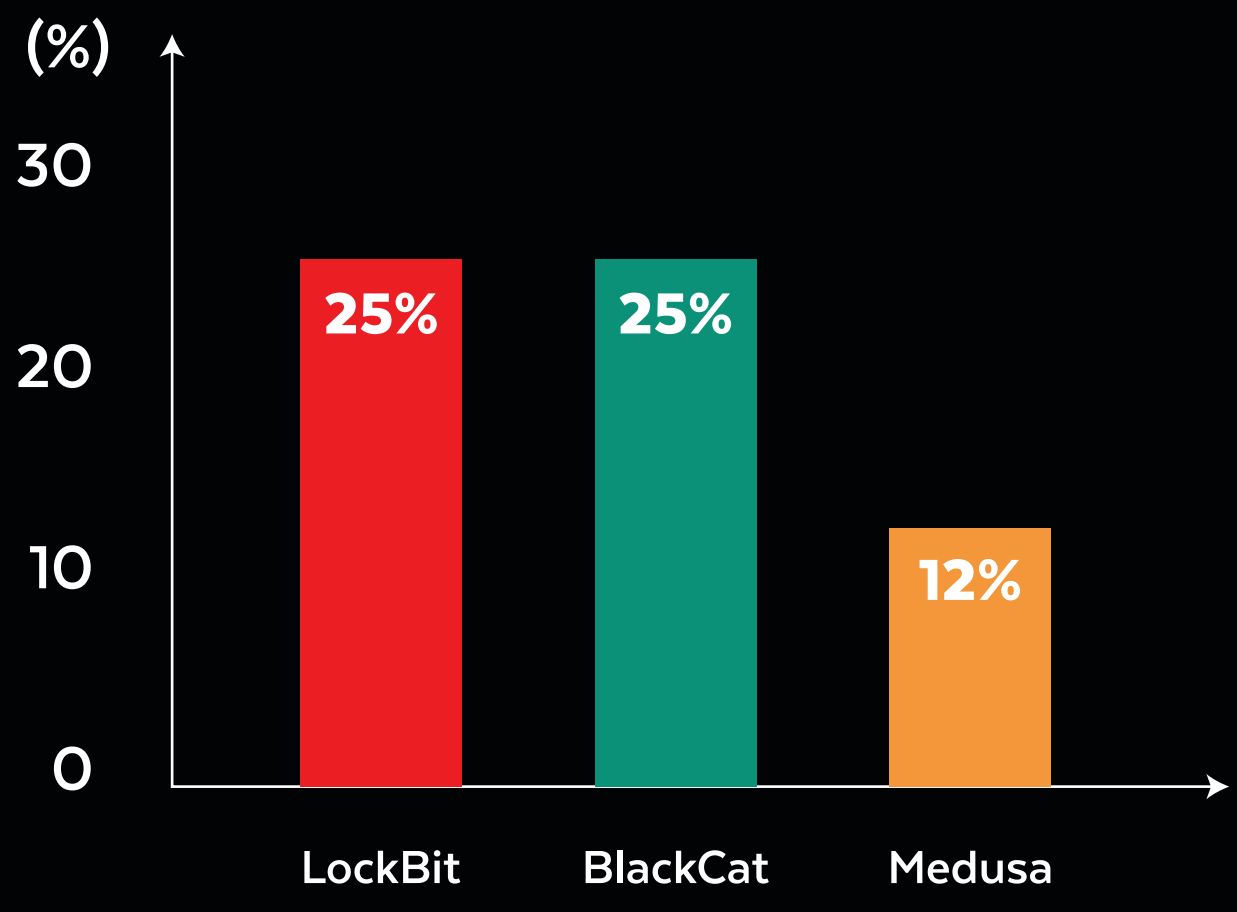
LEADING RANSOMWARE GROUPS OF 2023

RANSOMWARE ATTACKS ACROSS PAKISTAN

Over the past three years, several ransomware groups have targeted various sectors in Pakistan, with finance and industry being particularly affected. These attacks have paralyzed financial systems and encrypted critical information.

RANSOMWARE GROUPS NEUTRALIZED BY TISS

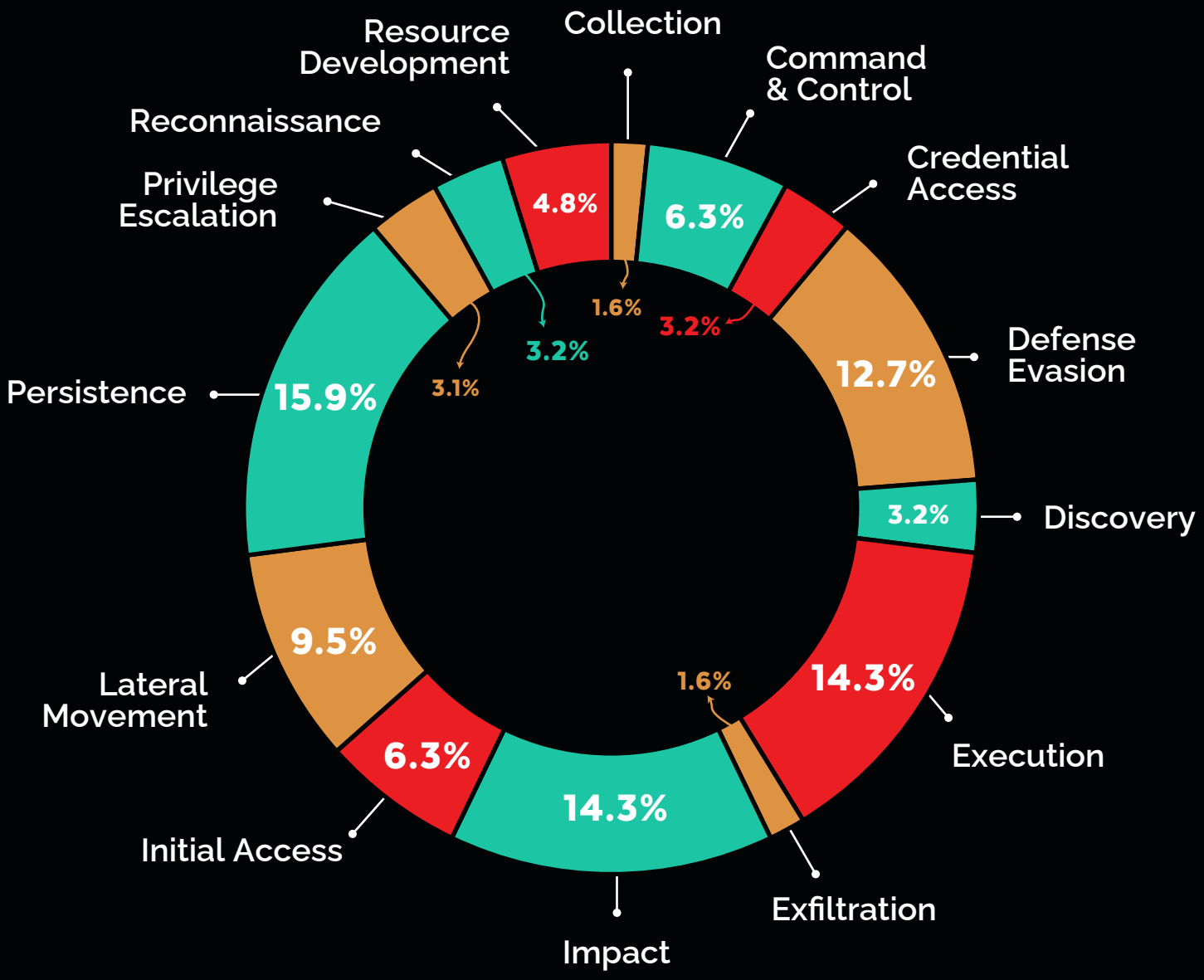
TISS has led Incident Response operations against major ransomware groups, including LockBit (25%), BlackCat (25%), and Medusa (12%). Our expertise has effectively minimized operational disruptions and preserved critical data integrity, enabling affected organizations to recover swiftly and resume normal business operations. We employ a multi-faceted approach to incident response: rapid threat identification, containment, eradication, and recovery. Using advanced tools and techniques.



COMMONLY USED MITRE TECHNIQUES IN CYBER ATTACKS

The MITRE ATT&CK framework serves as a structured repository of adversary tactics and techniques observed in cyberattacks. Developed by the MITRE Corporation, it categorizes threats into tactics representing adversary objectives and techniques representing specific methods to achieve those objectives.

Through analysis and investigation, Trillium Information Security Systems (TISS) has identified a range of Tactics, Techniques, and Procedures (TTPs) employed by threat actors. These include sophisticated methods such as Persistence (15.9%), achieved through Scheduled Tasks and Startup; Execution (14.3%), achieved by executing malicious payloads; Impact (14.3%), by halting critical services and encrypting important files; and Defense Evasion (12.7%), through Impersonation and Indicator Removal. By understanding these TTPs, organizations can develop effective mitigation strategies and strengthen their defenses against future attacks.



CONCLUSION

Reflecting on the insights from our Digital Forensics and Incident Response (DFIR) report, it's clear that the cyber threat landscape is both dynamic and relentless. TISS investigations have revealed a persistent trend of sophisticated cyberattacks, predominantly targeting high-value organizations. The Threat Pyramid framework offers a nuanced understanding of varying threat levels and impacts, enabling organizations to prioritize their defenses accordingly.

Our findings emphasize that the main causes of successful attacks often stem from the misconfiguration or non-implementation of critical security controls, such as Endpoint Detection and Response (EDR), user awareness programs, and effective patch management. By dissecting the tactics, techniques, and procedures (TTPs) employed by threat actors, TISS equips cybersecurity professionals with the knowledge to fortify their defenses. While achieving total security remains a formidable challenge, the practice of effective DFIR strategies can significantly mitigate risks and bolster organizational resilience.

Our aim in sharing this report is to empower organizations with the insights and tools necessary to proactively defend against cyber threats. As we navigate an increasingly perilous digital landscape, proactive measures, continuous vigilance, and collaborative efforts within the cybersecurity community are essential. This report serves as a resource, guiding organizations towards enhanced readiness and resilience against evolving cyber threats, fostering a safer digital environment for all.

35%
OF INCIDENTS LINKED TO ADVANCED PERSISTENT THREATS (APTS)

60%
OF CYBER ATTACKS TARGET HIGH-VALUE ORGANIZATIONS

35.7%
OF ALL INCIDENTS INVOLVE RANSOMWARE ATTACKS

TTPs BREAKDOWN

PERSISTENCE
15.9%

DEFENSE EVASION
12.7%

EXECUTION
14.3%