iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VII **Month of publication:** July 2025

DOI: https://doi.org/10.22214/ijraset.2025.73005

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

The Qilin(Agenda) Ransomware Campaign: Attack Vectors, Evasion Techniques, and Mitigation Strategies

Priyadarsana B[1], Priya P Sajan[2]
[1]*B.Tech, Department of CSE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, India*
[2]*Senior Project Engineer, C-DAC Thiruvananthapuram, India*

Abstract: ***Qilin ransomware was a sophisticated cyber-attack that targeted critical infrastructure systems in various locations around the world.***
The attacks were highly sophisticated. Qilin was able to bypass authentication and execute remote code using an unpatched vulnerability in Fortinet's second FortiGate and Fortisuite devices. The service offers Ransomware-as-As a Service with the ability to load any payload as required. This review paper examines the warhead dispatch mechanism, the evasion tactic, and a multi-phase extenuation and recovery technique.
Keywords: Qilin ransomware, Ransomware-as-a-Service (RaaS), Reflective DLL injection, Memory forensics, Fortinet vulnerability, Malware detection.

I. INTRODUCTION

In 2022, Qilin emerged as a Ransomware-based SaaS operation that offered advanced extortion tools to its affiliates. The ransomware can be distributed by accomplices in exchange for the money. More than 310 victims have been compromised by Qilin, with their information stolen from a secret website. Notable victims include: Yangfeng (Automotive),Lee Enterprises (Publishing), Court Services Victoria (Australia) and Synnovis (UK Pathology, NHS)

II. EXPLOITED VULNERABILITIES

The capabilities of Qilin and their ability to weaponise newly published vulnerabilities can be seen in a recent campaign, which exploited two important vulnerabilities for the Fortinet product. The operation makes use of CVE-2024-21762, a remote code execution vulnerability that was eventually patched in February 2025, and affected FortiOS and FortiProxy product lines. Based on what security specialists were able to assess, more than 150,000 vulnerable devices were still unpatched by March 2025, constituting a large attack surface.
The group has also reused CVE-2024-55591 which was an authentication bypass vulnerability that several advanced threat actors, including Mora_001, LockBit and SuperBlack ransomware operation had incorporated into their intrusion methodology. The reuse of vulnerabilities demonstrates how ransomware companies are continuing to share and reuse successful exploitation narrative within an ecosystem of cybercriminals.

III. ATTACK TACTICS AND PROCEDURES

Qilin's tactics follow a structured kill chain:
1) Gaining unauthorized access
2) Deploying ransomware payloads
3) Exfiltrating sensitive data
4) Encrypting endpoints and servers
5) Demanding ransom with threats of data leaks
These attacks are typically undetected until significant damage happens. Qilin may operate opportunistically and globally, but the region it is now focused on includes Spanish-speaking countries.

©IJRASET: All Rights are Reserved

IV. EXTENSIVE METHODS AND RESOURCES

A. Call Lawyer Feature

In 2025, Qilin added a "Call a lawyer" function to their ransom portal, creating a disguise of legal negotiation to pressure victims into faster payment decisions. This approach psychologically manipulates targets by creating a false impression of legitimate dispute resolution, which could prompt a hasty desire to cooperate.

B. Detection and Threat Analysis

Qilin ransomware samples submitted to VirusTotal are detected by over 60 vendors:

- Microsoft: *Ransom:Win32/QilinDecryptor.YTD!MTB*
- Fortinet: *W32/Filecoder_Kvilim.D!tr.ransom*
- BitDefender: *Gen:Variant.Ransom.Qilin.3*
- Some AV engines (e.g., Baidu, SentinelOne) failed to detect the threat.

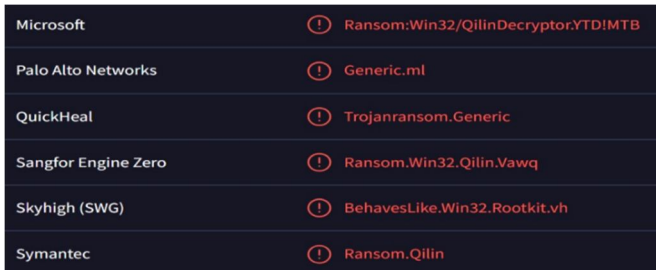


Fig 1: Detection labels assigned by various antivirus vendors for Qilin ransomware sample

The Fig 1. shows various antivirus vendors detecting Qilin ransomware under different threat signatures, such as Ransom:Win32/QilinDecryptor and Trojanransom.Generic.

V. LOADER AND DROPPER ANALYSIS

Qilin's operatives deploy a .NET-powered dropper known as NETXLOADER, which utilizes .NET Reactor v6 for code confusion to evade detection. It delivers SmokeLoader (intermediate malware) and Agenda ransomware (via reflective DLL injection). Evasion techniques include Control flow obfuscation, Just-in-Time (JIT) hooking and Meaningless method/function names

The ransomware primarily spreads through two initial access methods which is phishing campaigns or the exploitation of compromised legitimate credentials.

VI. TECHNICAL SOPHISTICATION

Key technical features include:

- AES-256 Encryption: Encrypted using CTR mode or ChaCha20.
- RSA-4096 Encryption: Used to encrypt the symmetric key per file
- Chrome Stealer Module: Extracts saved credentials.
- Self-Deletion: Deletes execution logs and itself to prevent forensics.
- Backup Corruption: Deletes shadow copies and backup registries.

VII. IMPACTED SECTORS

The following sectors mentioned in Table 1 has been impacted by this Qilin ransomware.

TABLE 1
IMPACTED SECTORS

Sector	Example Impact
Healthcare	NHS disruptions (Synnovis)
Publishing	Attack on Lee Enterprises
Government & Law	Breach of Court Services Victoria
Automotive	Yangfeng targeted
Finance/Retail	Victims in Spanish-speaking countries

©IJRASET: All Rights are Reserved

VIII. INCIDENT RESPONSE AND CONTAINMENT STRATEGY FOR QILIN RANSOMWARE

Standard file recovery is feasible, provided the need for a publicly available decryptor scheduled for Qilin's robust use of AES-256 and RSA-4096 encoding methods is satisfied. The report therefore proposes a thorough extinguishing procedure focusing on the containment of the threat, the preparation of the forensics for incident study, early detection of conduct, and the implementation of long-term precautionary measures to amplify structural adaptation.

A. Isolation and Containment

Infected endpoints should be reported immediately and removed from all network connectivity (including wired, wireless (Wi-Fi), and VPN), so that lateral movement ceases and further network injury is minimized. In addition to reducing access to affected systems, disabling certain services that malware common exploit to maneuver between systems is also recommended. These include Remote Desktop Protocol (RDP), which is a frequently exploited point for gaining remote access by attackers, and Server Message Block (SMB) which is convenient for file sharing, and access to network drives.

After a containment strategy has been employed, security teams should proceed to hunt and destroy known malicious binaries relating to the infection. One of these is PsExec, a legitimate remote administration tool that is very commonly abused by adversaries for malware procession and lateral movement, and w.exe, which is the payload of the Qilin ransom ware.

B. Volatile Memory Capture

In incident response, acquiring live memory is critical, especially when trying to recover volatile artefacts that are deleted or temporarily absent when the system shuts off like runtime configurations and decryption keys. For this purpose, we should ensure that we use leading memory forensic frameworks like Volatility and Rekall. The primary focus of the analysis will be extracting sensitive components, for example, RSA private keys, AES session keys, command-line arguments or configuration parameters that were passed during the malware run, etc. Because we will want to preserve all the volatile memory that may be useful for analysis, decryption attempts, or attribution, we must perform this task before shutting down the system.

C. Backup Verification

Recovery depends on the integrity of the backup. To search for Volume Shadow Copies you must first use vssadmin list shadows. When considering backups, also assess cloud backups (provided they weren't mapped during the attack) and offline backups (like disks or tapes) if there are no Volume Shadow Copy backups. Restore only after confirming the entire environment has been mitigated and patched.

D. File Structure Analysis

Analyzing encrypted files can provide useful information regarding the encryption methods used by the ransomware and can identify weaknesses. This includes looking at file headers and extensions to know if, for example, RSA-4096 is being used for key encapsulation purposes, or if strong algorithms like AES-256 in CTR mode (or ChaCha20) are being used to encrypt the data itself. While looking closely at the file structure, cryptographic weaknesses might reveal themselves, such as static IV reuse, AES key reuse across files, or incorrectly formed data blocks for the encrypted file. So far, there have not been any such implementation weaknesses identified in the Qilin ransomware samples examined.

E. RSA Key Testing

The ransomware-encrypted files may be decrypted if private key material is recovered, whether from memory captures or attacker tools. The original file content may be restored by attempting to decrypt AES key segments using programs like OpenSSL, CyberChef, or custom decryption scripts. This step is only possible if there is legitimate private key data in the disk artifacts or memory dump.

F. Behavioral Emulation

By controlled execution in a sandbox environment, you can analyze a ransomware behaviours and expose insider operational details. Analysts can gather further information about the potential purpose of malware by observing command-line parameters, such as --spread to enable network propagation, --password to unlock payload execution, and --no-local to omit local file encryption (this is typically only used for testing). The outcomes can then be used to generate Indicators of Compromise (IOCs) that could be integrated into SIEM environments, and YARA rules used for pattern-based detections.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

Any emulation exercise must be done completely in a closed lab environment using virtualization tools, either VMware or VirtualBox, to address the risks of unintentional spread and damage.

G. Defense Recommendations

Disable post-exploitation tools like PsExec and admin shares to improve incident response and stop infections in the future Implement EDR/XDR solutions that focus on fileless and memory-based attack detection. Patch as soon as possible; the Fortinet (e.g. CVE-2024-21762) and Veeam (e.g. CVE-2023-27532) vulnerabilities should be your top priorities. Implement offline, immutable, and regularly tested backups that are not available/visible to you (and your systems) during regular operations.. Keep an eye out for indicators of an attack, such as tampered PowerShell logs or mass file encryption.

IX. PROPOSED MITIGATION STRATEGY

Given the lack of a public decryptor for Qilin ransomware due to its strong use of AES-256 for file encoding and RSA-4096 for key encapsulation, the present work proposes a foresighted extenuation procedure focusing on untimely detection of fileless malware using memory forensics. Qilin is notable for its use of the brooding DLL injection technique, a method that allows the ransomware warhead to run entirely in memory without any drop artifact on the disk, thus excluding the classic antivirus and EDR mechanism.
To address this furtive execution method, we propose the development of a lightweight detection utility, designed to automate the acquisition, examination, and designation of an anomalous injection form associated with the brooding DLL load. The solution bridges the gap between the post-incident forensics investigation and the detection of real-time memory anomalies, enabling rapid response skills.

A. System Architecture and Workflow

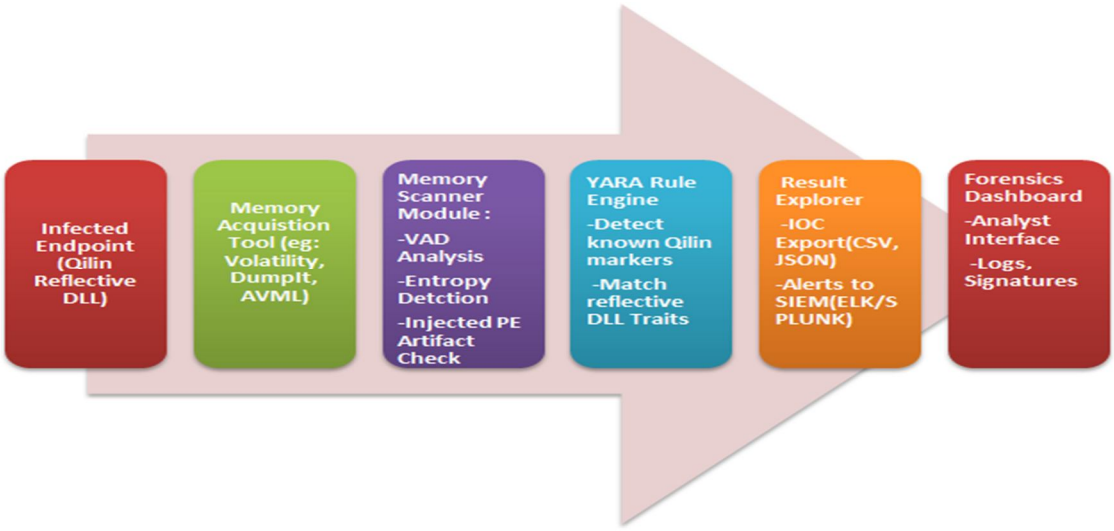


Fig. 2. System Workflow for Detection of Reflective DLL Injection by Qilin Ransomware

The proposed utility operates through the following detection pipeline:

1) Memory Acquisition: The device generates a certain memory retrieval utility, e.g. , WinPMEM or DumpIt to extract a packed RAM image of the suspected structure. This action continues unambiguous indications, including the injected code, active key, and the executed shell code, which otherwise drifts during the reboot.

2) Volatility-Driven Analysis: The RAM image is parsed using key Volatility plugins:

- malfind: Identifies suspicious VAD regions with execute permissions (PAGE_EXECUTE_READWRITE) and high entropy.
- ldrmodules: Compares loaded module lists against the PEB (Process Environment Block) to detect unmapped DLLs.
- dlllist: Lists all DLLs loaded by each process for correlation with ldrmodules.
- vadinfo: Inspects virtual memory regions, flags anomalies in access permissions and file mappings.

©IJRASET: All Rights are Reserved

3) Behavioral Signature Matching: This utility focuses on heuristics indicative of reflective DLL injection:
- Presence of PE headers (MZ, PE\0\0) in anonymous memory regions.
- DLLs not backed by file paths or missing from the PEB.
- High entropy (>7.0) memory blocks suggesting obfuscation or encryption.
- Inconsistencies between ldrmodules and dlllist, revealing injected but hidden DLLs.

4) IOC Extraction: Upon detection, this utility extracts key Indicators of Compromise (IOCs) to aid in forensic analysis and response. These include the process ID and parent-child process relationships, injected module base addresses and offsets, and any suspicious strings or YARA matches—such as ransom note fragments or loader function signatures. It also reports entropy scores and identifies anomalous memory protection flags, which may indicate obfuscation or unauthorized memory manipulation.

5) Reporting and Integration: For real-time alerts and a retrospective threat hunt, the results of the coverage and integration are transmitted in structured format (JSON, CSV) or, optionally, via the SIEM channels. This tool can be executed manually, or configured to run at an interval with Windows, Task Scheduler, or a cron job.

The Fig 2. demonstrates System Workflow for detection of Relative DLL Injection by Qilin Ransomware

B. Detection Heuristics Summary

TABLE 2
DETECTION HEURISTICS SUMMARY

Heuristic	Detection Plugin(s)	Description
High entropy memory regions	malfind, vadinfo	Suggest encrypted/packed payloads in RAM
PE headers in non-mapped VAD	malfind, yarascan	Indicates reflectively loaded PE modules
DLL present in malfind but missing in dlllist	ldrmodules, dlllist	Suggests stealth injection
Memory with PAGE_EXECUTE_READWRITE flags	vadinfo	Often abused for code injection
Unusual parent-child process chains	pstree, pslist	Evasion via trusted process hijacking

C. Real-World Use Case: Qilin Detection

Qilin has been seen utilising lateral movement strategies that make use of SMB and RDP, as well as remote administration tools like PsExec, to deploy its payload. Widespread, legitimate processes such as explorer.exe or svchost.exe are regularly reflectively injected with the ransomware payload; that is typically w.exe or a .dll variant nicknamed stevedore. Reflective injection is commonly overlooked by traditional antivirus applications due to it residing in memory only, executing under relevant process tokens, and utilizing string and command-line obfuscation to avoid detection.

Without using static signatures, the suggested utility finds these evasive methods by detecting hidden memory blocks not connected to known DLLs, identifying entropy spikes in specific memory regions, and searching for memory-resident ransom note strings and encryption routines.

D. Limitations and Future Enhancements

The tool has certain limitations even though it improves visibility into stealth ransomware behaviour. It is mostly reactive, necessitating memory capture following a suspected infection, which could postpone detection. Furthermore, false positives could occur, particularly in settings where red team exercises use authentic in-memory loaders like Cobalt Strike or Metasploit.

Future improvements are planned to fill in these gaps. These include detection capabilities for other stealth techniques like process hollowing, early bird injection, and APC injection; support for live memory scanning via tools like Volatility Live or EDR APIs; and integration with YARA rule sets that target known Qilin patterns. Additionally, SOC teams will be able to customise detection profiles to meet particular operational requirements thanks to a suggested plugin-based architecture.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

E. Impact and Novelty

This proposed utility has developed an automated memory-based warning system designed to detect brooding DLL injection, a major vector of modern ransomware, like Qilin. Unlike traditional antivirus scanners which are inactive, this scanner operates at the memory level, target files, and evasive malware procedures. The strategy must be fresh and sensible, donation forensics analyst, incident responder, and Blue Squads a targeted tool for capturing whatever traditional defenses they wish.

X. COMPARATIVE ANALYSIS WITH EXISTING MALWARE DETECTION TOOLS

The proposed tool is designed to detect memory-resident threats such as reflective DLL injections used by advanced ransomware strains like Qilin. In contrast to traditional antivirus and EDR tools, the proposed tool performs memory-level scanning to detect fileless malware during runtime. The following table presents a comparative analysis between the proposed tool and well-known detection solutions.

TABLE 3
COMPARISON OF PROPOSED TOOL WITH POPULAR MALWARE DETECTION SOLUTIONS

Feature / Tool	Proposed Tool (This Work)	Windows Defender ATP	Sysmon + SIEM	Volatility Framework	EDR (CrowdStrike, SentinelOne)
Detection Type	Memory-only (RAM forensics)	Signature-based + behavior monitoring	Logging + rule-based monitoring	Post-mortem memory analysis	Real-time behavioral + signature-based
Fileless Malware Detection	Yes, specialized for reflective DLLs	Limited	Depends on rule quality	Yes	Yes
Live Detection Capability	Near-real-time (scheduled scans)	Yes	No	No	Yes
Ransomware-specific Heuristics	Targeted for RaaS families	General detection only	Requires custom detection logic	No built-in heuristics	Some RaaS-specific modules
Memory Entropy and VAD Scanning	Yes (malfind, vadinfo, ldrmodules)	No	No	Yes	Partially supported
SIEM/ELK Integration	JSON, CSV, or Syslog output	Yes	Yes	Manual export needed	Native support
Internet Independent	Works offline	Needs connectivity	Depends on config	Fully offline	Cloud-dependent
Customizability / Extensibility	Plugin-based, YARA-compatible	Limited to Microsoft updates	Fully customizable	Supports scripts/plugins	Limited to vendor APIs
Specific Use-Case Fit for Qilin Ransomware	Tailored for in-memory ransomware	Not tuned to Qilin-specific behaviors	Needs IOC tuning	For forensic triage post-infection	If pre-configured for memory threats

The proposed tool effectively detects stealth-based and memory-only threats, such as those deployed by Qilin ransomware. Unlike standard AV and EDR platforms, which may overlook reflective DLL injection or encrypted in-memory payloads, the proposed tool focuses on entropy analysis, VAD mapping, and process injection anomalies. It acts as a complementary layer to existing endpoint defenses and fills a critical detection gap in modern ransomware defense.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

XI. CONCLUSION

The increasing complexity of ransomware threats is reflected in the Qilin campaign. A mature electronic menace landscape is represented by its use of furtive stevedores such as NETXLOADER, authorized manipulation techniques, and multi-stage infection mechanism. There are currently no decoding devices, so a layered defense method is essential. Organisations must establish patching, behaviour monitoring, direct entry, and backup procedures to protect against such advanced attacks.

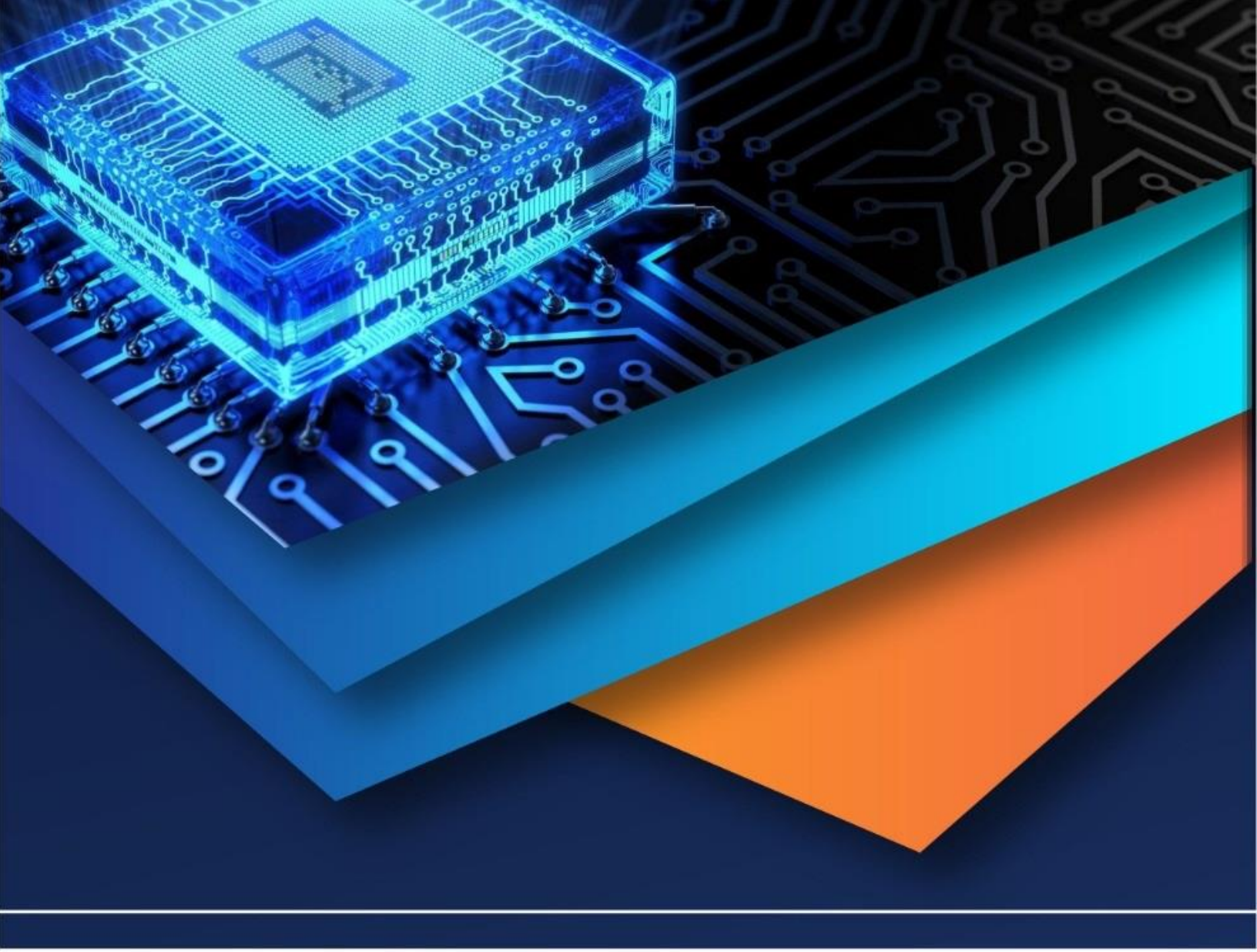
XII. ACKNOWLEDGEMENT

For the opportunity and assistance given during this project, the author would like to sincerely thank the Centre for Development of Advanced Computing (C-DAC), Thiruvananthapuram. We would especially like to thank Mrs. Priya P. Sajan, Senior Project Engineer, for her invaluable advice, technical know-how, and unwavering support during the completion of this work.

REFERENCES

[1] Fortinet, Fortinet PSIRT: CVE-2024-21762 - Remote Code Execution in FortiOS and FortiProxy, Feb. 2025. [Online]. Available: https://www.fortiguard.com/psirt/FG-IR-24-00162
[2] Veeam, CVE-2023-27532: Vulnerability in Backup & Replication - Sensitive Information Disclosure, Veeam Security Advisory, 2023. [Online]. Available: https://www.veeam.com/kb4424
[3] MITRE ATT&CK, “Enterprise Techniques: Initial Access, Privilege Escalation, Defense Evasion,” MITRE Corporation, 2024. [Online]. Available: https://attack.mitre.org
[4] Group-IB, Qilin Revisited: Diving into the techniques and procedures of the recent Qilin Ransomware Attacks, July 2024. [Online]. Available: https://www.group-ib.com/blog/qilin-ransomware-analysis
[5] Mandiant, Best Practices for Ransomware Defense, FireEye Intelligence Report, vol. 37, 2024.
[6] A. Caseley et al., “Detection of Reflective DLL Injection via Memory Forensics,” Proc. 17th Conf. Digital Forensics Research Workshop (DFRWS), 2023, pp. 19–30.
[7] Volatility Foundation, Volatility 3 Framework Documentation, 2024. [Online]. Available: https://volatility3.readthedocs.io
[8] S. Stojanovic, “Combating Ransomware Through Fileless Malware Detection: A Memory-Only Approach,” IEEE Transactions on Information Forensics and Security, vol. 19, pp. 1311–1325, Mar. 2024.
[9] Microsoft, PsExec Utility - Sysinternals Suite, Microsoft Docs, 2024. [Online]. Available: https://docs.microsoft.com/sysinternals/downloads/psexec
[10] D. L. Johnson and T. Moore, “Cryptographic Implementation Failures in Ransomware Payloads,” ACM Transactions on Privacy and Security, vol. 27, no. 2, Apr. 2023.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)