
CAPSTONE PROJECT

KEY LOGGER AND SECURITY

Presented By:

**Yamini N-University College of Engineering, Kanchipuram-
Computer Science and Engineering**

OUTLINE

- Problem Statement
- Proposed System/Solution
- System Development Approach
- Algorithm & Deployment
- Result (Output Image)
- Conclusion
- Future Scope
- References

PROBLEM STATEMENT

- ✓ Advanced Evasion Techniques: APT actors employ sophisticated evasion techniques, such as polymorphic malware, encrypted communication channels, and zero-day exploits, to bypass traditional security defenses and remain undetected within network environments.
- ✓ Insider Threats and Compromised Credentials: A significant proportion of APT incidents involve insider threats or compromised credentials, either through social engineering tactics or insider collusion. Traditional security measures struggle to differentiate between legitimate user activities and malicious behavior initiated by insiders or compromised accounts.
- ✓ Lack of Comprehensive Threat Intelligence: Effective defense against APTs requires timely and accurate threat intelligence to identify emerging attack vectors, tactics, and indicators of compromise (IOCs). However, many organizations lack the necessary resources and capabilities to gather, analyze, and act upon relevant threat intelligence effectively.

PROPOSED SOLUTION

✓ Threat Intelligence Platform (TIP):

- Implement a centralized Threat Intelligence Platform to aggregate, correlate, and analyze threat intelligence from various internal and external sources.
- Utilize machine learning algorithms and natural language processing to automate threat intelligence processing and enrich indicators of compromise (IOCs) with context.
- Enable real-time dissemination of actionable threat intelligence to security controls and personnel for timely threat detection and response.

✓ Next-Generation Endpoint Protection:

- Deploy advanced endpoint protection solutions powered by machine learning, behavioral analysis, and threat intelligence integration to detect and prevent APT-related activities.
- Implement endpoint detection and response (EDR) capabilities for continuous monitoring, threat hunting, and forensic analysis of endpoint activity to identify and mitigate APT attacks.

✓ Network Segmentation and Micro-Segmentation:

- Segment the network into distinct zones based on risk profiles, data sensitivity, and business functions to limit lateral movement and contain APT propagation.
- Implement micro-segmentation using software-defined networking (SDN) or virtualization technologies to enforce granular access controls and isolate critical assets from potential APT infiltration.

SYSTEM APPROACH

The "System Approach" section outlines the overall strategy and methodology for developing and implementing the rental bike prediction system. Here's a suggested structure for this section:

- Security Architecture
- Risk management framework

ALGORITHM & DEPLOYMENT

❑ Encryption Algorithms:

- Symmetric Encryption: AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple DES)
- Asymmetric Encryption: RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography)

❑ Hashing Algorithms:

- Secure Hash Algorithm (SHA-256, SHA-3)
- Message Digest Algorithm (MD5)

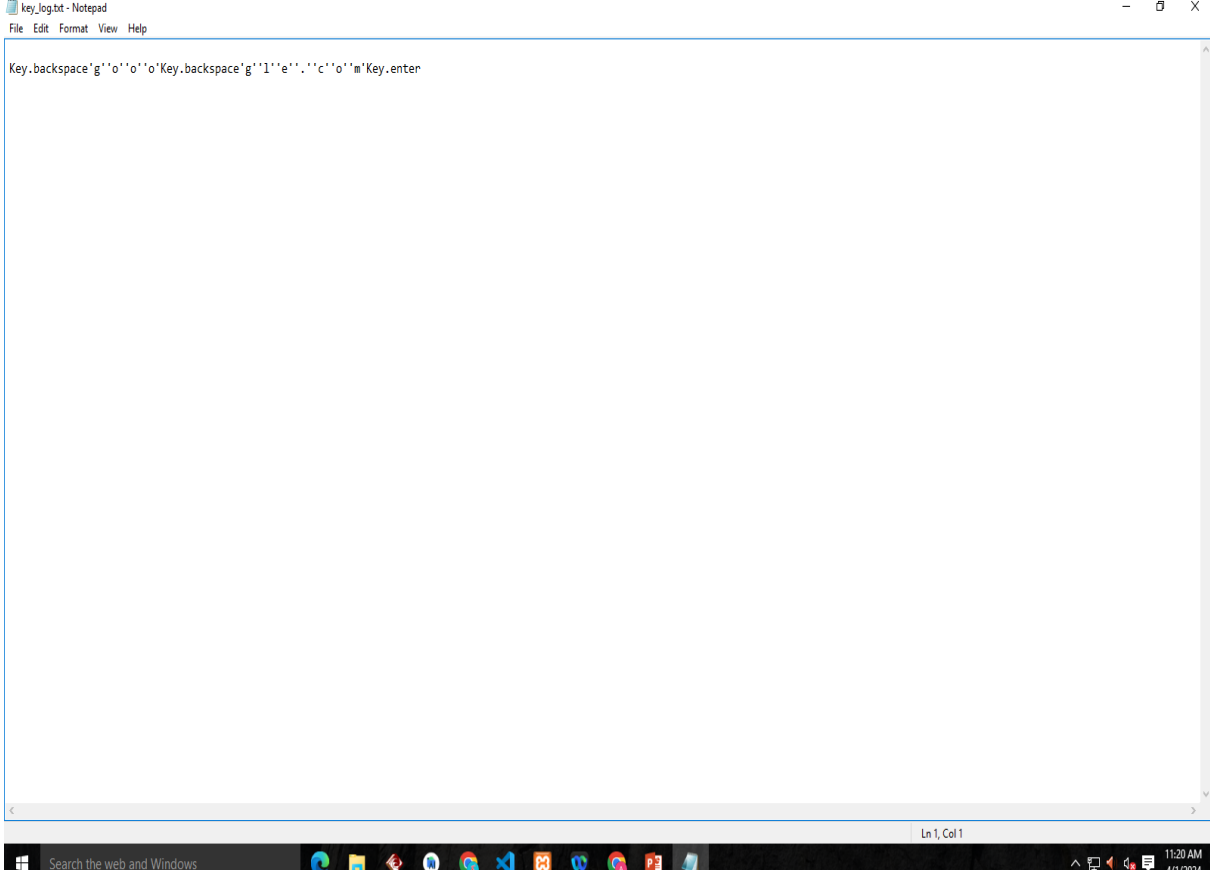
❑ Key Exchange Algorithms:

- Diffie-Hellman Key Exchange
- Elliptic Curve Diffie-Hellman (ECDH)

❑ Digital Signature Algorithms:

- RSA Digital Signature
- Elliptic Curve Digital Signature Algorithm (ECDSA)

RESULT

[illegible]

key_log.txt - Notepad

File Edit Format View Help

Key.backspace'g''o''o''o'Key.backspace'g''l''e'', ''c''o''m'Key.enter

Ln 1, Col 1

Search the web and Windows

11:20 AM
4/1/2024

CONCLUSION

Key loggers represent a potent and insidious threat in the realm of cybersecurity, capable of stealthily capturing sensitive information, compromising user privacy, and facilitating various forms of cybercrime. As technology continues to advance, key loggers evolve in sophistication, making them challenging to detect and mitigate. Therefore, understanding key loggers and implementing robust cybersecurity measures are imperative for safeguarding individuals and organizations against these threats.



THANK YOU