VAJJI MANOHAR

Threat Researcher | Cybersecurity Professional

manohar777vajji@gmail.com 9640942134 Hyderabad, Telangana

https://www.linkedin.com/in/vajji-manohar-239431208

Profile

Cybersecurity professional with **3+ years** of hands-on experience in **malware analysis**, **threat research**, and **EDR operations**. Skilled in utilizing various tools for **static** and **dynamic analysis**, **reverse engineering**, and **vulnerability assessments**. Adept at improving **detection quality** and reducing **false positives** in **EDR systems**. Seeking a challenging role to drive business growth while enhancing cybersecurity capabilities.

Professional Experience

Threat Researcher, *LTI Mindtree* 06/2021 – 10/2024 | Hyderabad, India

- Conducted in-depth **static** and **dynamic analysis** on over 200+ **malware samples** to identify **IOCs**, behaviors, and capabilities.
- Reverse-engineered **PE**, **APK**, **Linux**, **Android**, and **Macro files** to extract critical **indicators**.
- Contributed to the development and optimization of **EDR systems** by analyzing 100+ **alerts** for **quality assurance** and fine-tuning **detection accuracy**.
- Developed and implemented 50+ **static** and **generic signatures** to detect **malware** and suspicious files.
- Reduced **false positives** by **30%** through fine-tuning **EDR suppression rules** and enhancing **machine event data analysis**.
- Provided **IOCs** and **TTPs** for **threat hunting** initiatives, supporting proactive detection efforts.
- Worked closely with the **Windows Defender (EDR)** team to test new **detectors** and evaluate **telemetry** before deployment.

Skills

Malware Analysis & Reverse Engineering
Proficient in **static** and **dynamic analysis** of **malware samples**.

Security Research
In-depth knowledge of **threat hunting**, **signature tuning**, and providing **IOCs** & **TTPs**.

Programming
Familiar with **interpreted** and **compiled programming languages** for **reverse engineering**.

EDR Operations
Expertise in **Microsoft Defender Advanced Threat Protection** and tuning **EDR alerts** for improved **detection quality**

Cryptography & Web Application Security
Strong understanding of **cryptography** principles and **web app security** vulnerabilities.

Vulnerability Assessment
Experience conducting **vulnerability assessments** in **embedded systems** and **applications**.

Projects

Microsoft Project, *Malware Analysis*
Conducted **in-depth malware analysis** using tools like **CFF Explorer**, **PEView**, **PEStudio**, **HexView**, **PEID**, **Die**, **Procmon**, **Regshot** and **Wireshark** to identify IOCs, behaviors, and network patterns. Performed **static** and **dynamic analysis** on 200+ samples, uncovering malicious capabilities and obfuscation techniques. Developed 50+ **detection signatures**(**Static Signatures and BM Signatures**)for improved threat defense

Microsoft Project, *Cross-Plat form and Reverse engineering*
Performed **cross-platform malware analysis** and **reverse engineering** on Windows, Linux, and Android samples using tools like **PEStudio**, **HexView**, **Procmon, Process Monitoring, Process Explorer**, **Regshot**and **Wireshark**. Identified vulnerabilities and malicious behaviors across multiple OS environments. Developed tailored detection signatures(**Static and Gneric Signatures for Microsoft Defender**) for enhanced **EDR** and proactive threat defense.

Microsoft Project, *EDR(Endpoint Detection and Response)*
Led an **EDR project** focused on analyzing **Microsoft Defender ATP** alerts, fine-tuning suppression rules, and reducing **false positives**(**Rasing bugs for the better quality**) by 30%. Conducted in-depth analysis of 100+ alerts, improving detection accuracy and quality. Collaborated with the team to test and deploy new **EDR detectors** for enhanced threat detection

Operating System and Network Fundamentals
Completed a project on **Operating System** and **Network Fundamentals**, focusing on system resource management, process scheduling, and network protocols. Configured and analyzed **TCP/IP** communication and **network traffic** using tools like **Wireshark**. Developed practical insights into **OS internals** and **network troubleshooting** for enhanced system performance and security

Cryptography and Application Security
Developed a project on **Cryptography** and **Application Security**, focusing on encryption algorithms, key management, and secure data transmission. Implemented **SSL/TLS** protocols and vulnerability assessments to identify and mitigate application security risks. Conducted real-world testing on web applications to enhance **secure coding practices** and **data protection**

Certificates

edureka:
Certified Ethical Hacker (CEH)

Education

Electronics and Communication Engineering, 04/2015 – 05/2019 | Vizag, India
Pydah College of Engineering and Technology
Percentage: 80%