Mayank Malik

mayankmalik012@gmail.com | linkedin.com/in/mostwanted002 | gitlab.com/mostwanted002 | github.com/mostwanted002

Technical Skills

Languages: C/C++, Python, Java, GO, PHP
OS: Windows, Linux, Android
Analysis & other Tools: Ghidra, IDA Pro, x64dbg, windbg, Git, Docker, Google Cloud Platform, VS Code, Visual Studio, APKLab, apktool, radare2, Hyper-V, VMWare, Proxmox, OpnSense
Frameworks & EDR: ElasticSearch, Kibana, Logstash, SentinelOne, CarbonBlack, Microsoft Defender, Crowdstrike

Experience

Security Researcher II – Adversary Emulation (VANQUISH DETECTIONS) Nov 2025 – Present
Microsoft India (R&D) Pvt. Ltd. *Hyderabad, India*

- Conducted research driven emulation and analysis of Web-shell based attacks and post-exploitation scenarios on Windows Server to measure existing detection efficacy and identify gaps & opportunities at scale across M365 Infrastructure
- Performed statistical analysis of top threat actors' tactics and procedures to have a comparative result against existing security posture across M365 and Microsoft.
- Provided key insights and emulation derived data with crucial telemetry to fellow researchers and engineers for fast tracking from detection ideas to detection deployment.

Threat & Malware Analyst - Incident Response Nov 2021 – Nov 2025
Certego SRL *Modena, Italy*

- Conducted in-depth analysis of malware samples to identify their origins, functionality, and potential impact on systems
- Reverse-engineered malicious code using tools such as IDA Pro and x64dbg to understand the behavior and implement countermeasures
- Created lab environment for independent threat and malware investigation for PCs and mobile platform
- Developed and maintained malware analysis reports, documenting findings and recommendations for mitigation
- Stayed updated with the latest malware trends, APT activities, vulnerabilities, and attack techniques to enhance the organization's security posture
- Engaged in studying the threat landscape, to optimize the detection capabilities of the Certego PanOptikon platform
- Engaged in analysis and response to IT incidents on Customer networks
- Collaborated with incident response teams to investigate and respond to security incidents, providing expertise in malware analysis

Threat Analyst Dec 2020 – Nov 2021
Netenrich Inc. *Bangalore, India*

- Engaged in attack surface monitoring and superficial penetration testing for multiple clients
- Participated in vulnerability assessments and penetration tests to identify potential weaknesses and gaps in security controls
- Assisted in the development and implementation of security policies, procedures, and controls to enhance the organization's overall security posture

Projects

fork-bomb-win | *C, Windows* Dec 2023

- Developed a PoC that immitates 'fork()' system call on windows and renders the system unusable

rffuzzer | *GO, Web Applications* Aug 2021

- Developed a HTTP Header fuzzing utility to determine if any of the headers are vulnerable to SSRF

exfiltrace | *GO, Linux* June 2020

- Developed a data exfiltration client-server tool

- Incorporates a custom encryption similar to TLS for establishing a channel and sending data from client to server

datanoid | *python, Linux* Jan 2019

- Developed a multi-level data obfuscation and encryption tool
- Incorporates a combination of Caesar's Cipher combined with AES-128-CBC encryption and RSA-2048 of key encryption

Education

University of Delhi New Delhi, India

Bachelor of Science (Honors) in Computer Science *Jul 2017 – Oct 2020*

Shardein School Muzaffarnagar, India

Class XII CBSE *May 2016 – May 2017*