

Mayank Malik

C RTP | Incident Responder | Malware and Threat Analyst | Security Researcher

<https://mostwanted002.page/>

<https://www.linkedin.com/in/mostwanted002>

Based in Uttar Pradesh, India

Highly skilled and dedicated malware analyst with 1 year of experience in incident responding, analyzing, detecting, and mitigating malware threats. Seeking a challenging position as a malware analyst to utilize my expertise in identifying and neutralizing complex malware attacks to ensure the security and integrity of computer systems.

Summary of Qualifications

- Extensive knowledge of malware analysis techniques, tools, and methodologies.
- Proficient in reverse engineering malware samples to identify their functionality and behavior.
- Strong understanding of various malware types, including viruses, worms, Trojans, ransomware, and botnets.
- Experience in analyzing network traffic, logs, and system behavior to detect and investigate potential security incidents.
- Skilled in using industry-standard tools such as IDA Pro, x64dbg, Wireshark, and YARA.
- Familiarity with different operating systems, including Windows, macOS, and Linux.
- Excellent problem-solving and analytical skills, with a keen eye for detail.
- Effective communicator and collaborator, able to work well in cross-functional teams.

Professional Experience

Threat Analyst and Incident Responder

Certego SRL, Modena, Italy

November 2021 - Present

- Engaged in analysis and response to IT incidents on Customer networks
- 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.
- Collaborated with incident response teams to investigate and respond to security incidents, providing expertise in malware analysis.
- Developed and maintained malware analysis reports, documenting findings and recommendations for mitigation.
- Stayed updated with the latest malware trends, vulnerabilities, and attack techniques to enhance the organization's security posture.
- Engaged in studying the threat landscape, in order to optimize the detection capabilities of the Certego PanOptikon platform

Threat Analyst

Netenrich Inc., Bangalore, India

December 2020 - November 2021

- 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.
- Stayed up to date with the latest threats, vulnerabilities, and security technologies through continuous learning and industry conferences.

Education

- **Bachelor's of Science (Honors)
Computer Science**

6.9 CGPA (on a scale of 10)

University of Delhi

2017-2020

Publications

- **CVE-2020-13379**

A new attack scenario was found in Grafana, that lead to Application Level Denial of Server
- **Conti Locker Analysis**


A breakdown and cryptanalysis of the famous ransomware “Conti Locker” created by the APT group “Conti”
- **Malware Analysis and Triage Report : PirateStealer**

Analysis and Triage Report of an info-stealer equipped with VM Detection and Evasion


Certifications

- **Practical Malware Analysis and Triage**, September 2022


TCM Security

[Certificate](#) 
- **Certified Red Team Professionals**, April 2021


Pentester Academy

[Certificate](#) 
- **Autopsy 8-Hour Online Training**, June 2020


Basis Technology

[Certificate](#) 
- **Security in Google Cloud Specialization**, November 2020


Coursera

[Certificate](#) 
- **Architecting with Google Kubernetes Engine**, July 2020


Coursera

[Certificate](#) 
- **Architecting with Google Compute Engine**, September 2019





Coursera

[Certificate](#) 
- **12 Badges, 205 Exercises**

PentesterLab

[Profile](#) 

Projects

- **RFFuzzer** 
Simple SSRF Fuzzer to detect SSRF Injection via HTTP Headers
- **Exfiltrace** 
An encrypted data exfiltration server-client application for Red Teaming.
- **Datanoid** 
Datanoid (release v2.0) is a CLI based Python Script which provides three-level encryption.
- **TheNotebook** 
Vulnerable machine submitted to HackTheBox platform.

Languages

- English (Fluent)
- Hindi (Native)

Achievements

- Hall of Fame at Healthify Me, Oracle, Comcast, IKEA, Garfana on BugCrowd and hackerone