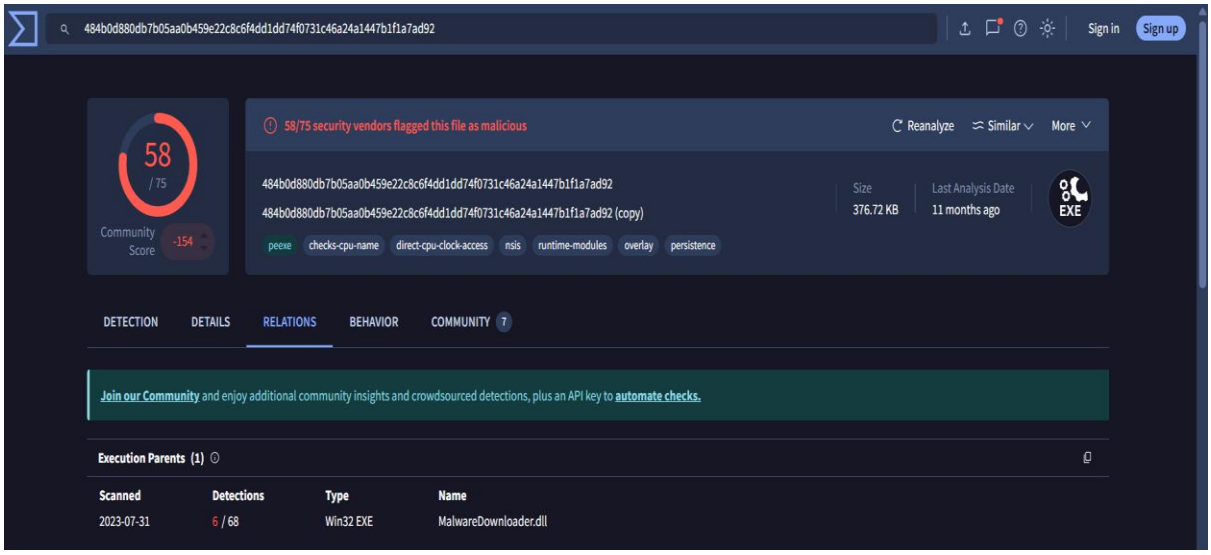
Name : Sandhya Singh

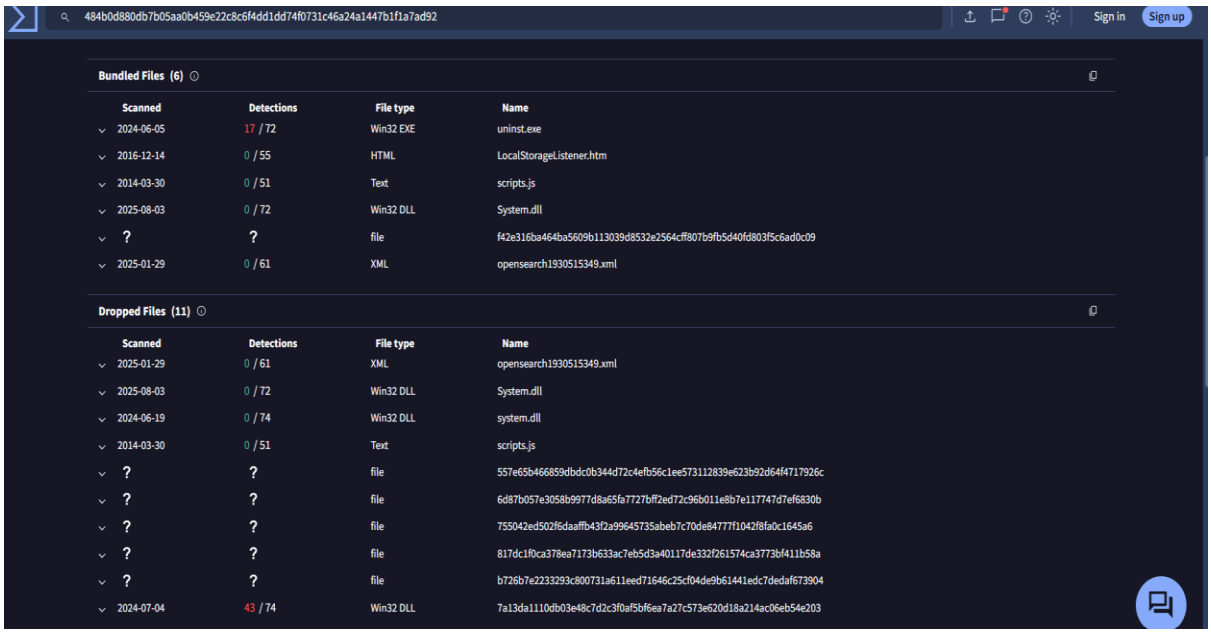
Intern ID : 233

Malware Analysis

HW32.Packed HW32.Packed

Hash : 484b0d880db7b05aa0b459e22c8c6f4dd1dd74f0731c46a24a1447b1f1a7ad92





📄 Practical Activity: Investigating Suspicious Foreign Address

---

🔷 Activity Name:

Finding ISP and Related Information of a Suspicious Foreign Address

---

🎯 Objective:

To find the ISP and location of a suspicious foreign address using online Whois tools for further investigation.

🧪 Tools Used:

- Whois tools (Online tools)
- Robtex
- Web Browser (Google Chrome)

📋 Steps Performed:

1. **Opened Whois Tools Website:**
    - Launched web browser.

- Navigated to an online Whois lookup site (e.g., https://whois.domaintools.com).

2. **Entered Suspicious IP Address:**
   - Copied the suspicious foreign address (IP or domain) detected during malware analysis.
   - Pasted it into the Whois lookup tool.
3. **Analyzed Whois Results:**
   - Collected information such as:
     - ISP (Internet Service Provider)
     - Hosting Provider
     - Country and City location
     - Contact details (Abuse contact if available)
4. **Verified on Robtex:**
   - Opened https://www.robtex.com.
   - Entered the same IP/domain.
   - Cross-checked additional data like DNS records, routing paths, related domains, and network blocks.
5. **Documented Findings:**
   - Noted down all relevant findings.
   - Highlighted any unusual or suspicious details such as:
     - Known malicious ISP
     - Hosting in high-risk countries
     - Domains associated with previous malware campaigns

📝 **Conclusion:**

- The ISP and geolocation of the suspicious foreign address were successfully identified.
- This information helps in understanding the origin of the threat and supports deeper malware investigation and reporting.

If you want, I can also prepare a **final combined version** of both activities:

1. Malware Hash Analysis
2. Suspicious Foreign Address Investigation

Just reply **“Combine both”** if you'd like.

Ask ChatGPT