

Name : Sandhya Singh

Intern ID : 233

## Malware Analysis

HW32.Packed HW32.Packed

Hash : 484b0d880db7b05aa0b459e22c8c6f4dd1dd74f0731c46a24a1447b1f1a7ad92

Community Score: 58 / 75

58/75 security vendors flagged this file as malicious

File Details:

- 484b0d880db7b05aa0b459e22c8c6f4dd1dd74f0731c46a24a1447b1f1a7ad92
- 484b0d880db7b05aa0b459e22c8c6f4dd1dd74f0731c46a24a1447b1f1a7ad92 (copy)

File Type: Win32 EXE

Size: 376.72 KB | Last Analysis Date: 11 months ago

Tags: pdee, checks-cpu-name, direct-cpu-clock-access, nsis, runtime-modules, overlay, persistence

Execution Parents (1):

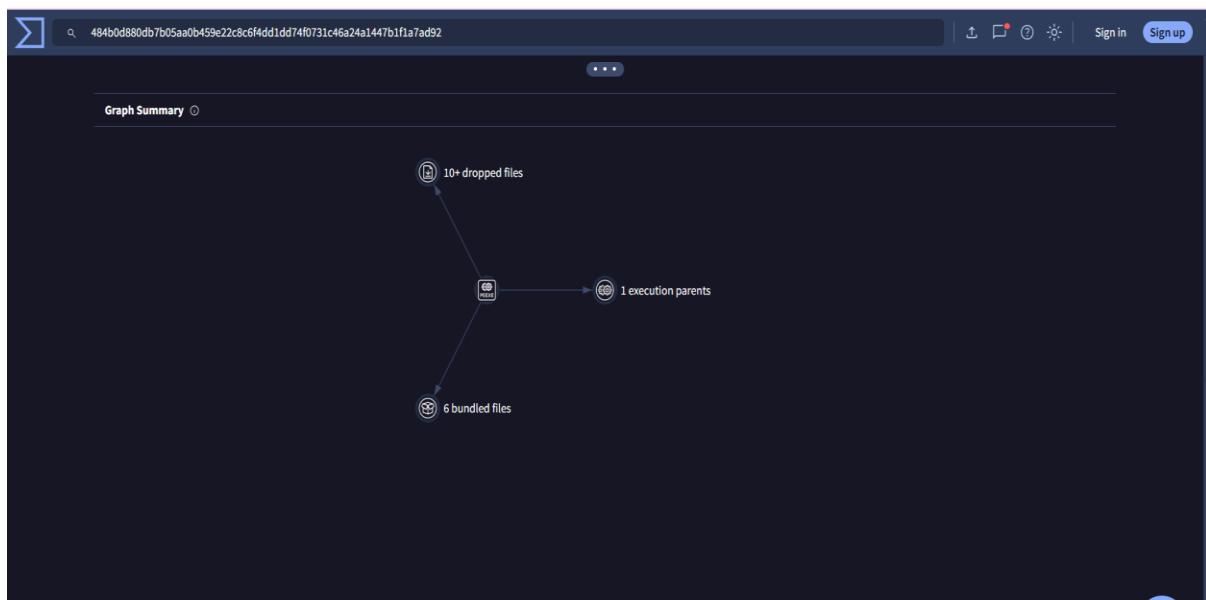
Scanned	Detections	Type	Name
2023-07-31	6 / 68	Win32 EXE	MalwareDownloader.dll

Bundled Files (6):

Scanned	Detections	File type	Name
2024-06-05	17 / 72	Win32 EXE	uninst.exe
2016-12-14	0 / 55	HTML	LocalStorageListener.htm
2014-03-30	0 / 51	Text	scripts.js
2025-08-03	0 / 72	Win32 DLL	System.dll
?	?	file	f42e316ba464ba5609b113039d8532e2564cff807b9fb5d40fd803f5c6ad0c09
2025-01-29	0 / 61	XML	opensearch1930515349.xml

Dropped Files (11):

Scanned	Detections	File type	Name
2025-01-29	0 / 61	XML	opensearch1930515349.xml
2025-08-03	0 / 72	Win32 DLL	System.dll
2024-06-19	0 / 74	Win32 DLL	system.dll
2014-03-30	0 / 51	Text	scripts.js
?	?	file	557e65b466859dbdc0b344d72c4efb56clee573112839e623b92d64f4717926c
?	?	file	6d87b057e3058b9977d8a65fa7727bf2ed72c965011e8b7e117747d7ef6830b
?	?	file	755042e502f6daaffb43f2a9964573abeb7c70de84777f1042f8f0c1645a6
?	?	file	817dc1f0ca378ea7173b633ac7eb5d3a40117de332f261574ca3773bf411b58a
?	?	file	b726b7e2233293c800731a611eed71f646c25cf04de9b61441edc7dedaf673904
2024-07-04	43 / 74	Win32 DLL	7a13da1110db03e48c7d2c3f0a5bf6ea7a27c573e620d18a214ac06eb54e203



## 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