Aim:

IT audit for the **Parivahan** Government website's information system to analyse malware and do vulnerability assessments.

Tools:

We conducted a malware analysis and vulnerability assessment using the following tools:

1) "**Hybrid"** for software analysis

2) **Pentest** vulnerability scanning tool

Procedure:

The procedure of malware analysis is:

- **Static properties analysis** - Analyse the properties include the strings embedded into the file, header details, hashes, embedded resources, packer signatures, metadata such as the creation date, etc.
- **Interactive behaviour analysis** - Used to observe and interact with a malware sample running in a lab. Analysts seek to understand the sample's registry, file system, process and network activities
- **Fully automated analysis** - Use the input of various resources to automate the management of operations and information, creating useful output that can help a company make strategic decisions.
- **Manual code reversing** - Decoding encrypted data stored or transferred by the sample. Determining the logic of the malicious program's domain generation algorithm.

Methodology:

Malware analysis:

We conducted an analysis using the "**Hybrid"** Analysing Tool to do a follow-up analysis.

File Verification: We verify that the development files of the websites have not been tampered with or modified since they were last signed or verified.

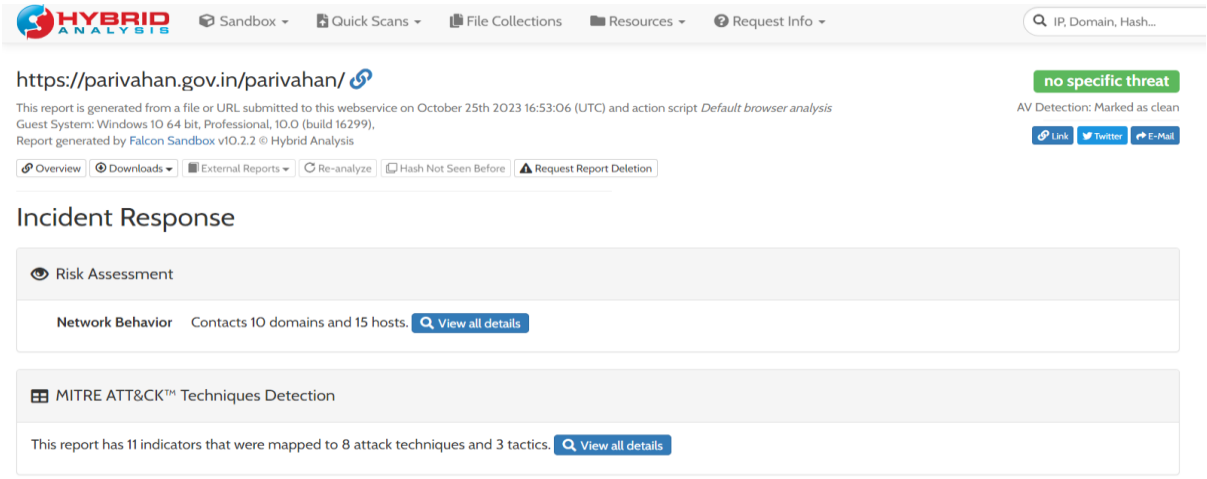
Imports and Exports Analysis: The tool provides information about the imports and exports used by the file, including the functions and libraries used.

This analysis gives the results of the following malware on the **Parivahan** website:

Spyware: Collects user activity data without their knowledge.

Adware: Serves unwanted advertisements

Trojans: disguise themselves as desirable code.



Vulnerability Assessment:

The scan was conducted using the **Pentest** Professional vulnerability scanning tool for the **Parivahan** website's information systems. By utilizing this scanning tool inside the network perimeter along with valid domain credentials is to bypass existing external security controls and host-based security measures to gain a detailed look at system configuration and patch levels. The 00.00.00.0/00 subnet was identified by the toll, with further specification to scan hosts residing in the **Parivahan** website's domain.

The vulnerability scan occurs in two phases:
1. Network Discovery
2. Vulnerability Assessment

The network discovery phase is conducted to discover live hosts on the target network and involves various host discovery methods such as ICMP pings, ARP pings, and TCP connections to well-known ports. The vulnerability assessment uses data gathered during the first phase to generate the report.

Vulnerabilities found for server-side software

CVSS	CVE	SUMMARY	EXPLOIT	AFFECTED SOFTWARE
4.3	CVE-2016-10735	In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.	N/A	bootstrap 3.3.5
4.3	CVE-2018-14040	In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.	N/A	bootstrap 3.3.5
4.3	CVE-2018-14042	In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.	N/A	bootstrap 3.3.5
4.3	CVE-2018-20676	In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.	N/A	bootstrap 3.3.5
4.3	CVE-2018-20677	In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.	N/A	bootstrap 3.3.5

Risk description

These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Recommendation

We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Insecure cookie setting: missing Secure flag

URL: https://parivahan.gov.in/parivahan/

COOKIE NAME: SERVERID_parivahan_73

EVIDENCE: Set-Cookie: SERVERID_parivahan_73=parivahanapp5; path=/

Risk description

Since the `Secure` flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, the risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation

Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Insecure cookie setting: missing HttpOnly flag

URL: https://parivahan.gov.in/parivahan/

COOKIE NAME: SERVERID_parivahan_73

EVIDENCE: The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag: Set-Cookie: SERVERID_parivahan_73=parivahanapp5

Risk description

A cookie has been set without the `HttpOnly` flag, which means that it can be accessed by the JavaScript code running inside the web page. If an attacker manages to inject malicious JavaScript code on the page (e.g. by using an XSS attack) then the cookie will be accessible and it can be transmitted to another site. In case of a session cookie, this could lead to session hijacking.

Recommendation

Ensure that the HttpOnly flag is set for all cookies.

Missing security header: Referrer-Policy

URL: https://parivahan.gov.in/parivahan/

EVIDENCE: Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.

Risk description

The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application. For instance, if a user visits the web page "http://example.com/pricing/" and it clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation

The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

Executive Summary

The purpose of this vulnerability scan is to gather data on Windows and third-party software patch levels on specified hosts in the domain. The audit was performed on "**2023-10-25**" using **Pentest vulnerability scan** Tool.

Of the 14 hosts identified, 32 systems were found to be active and were scanned. A total of 5 unique vulnerabilities were found during this scan. Critical, high, and medium severity vulnerabilities were found to exist across all 32 systems.

The vulnerabilities found on Windows hosts consist of outdated Windows patches and third-party software including Google Chrome and Adobe Flash. Systems were also found to be missing patches from 2014. Older vulnerabilities present a more significant risk as malicious actors will often automate exploitation of known vulnerabilities in an attempt to catch the lowest hanging fruit.

Therefore, we strongly recommend applying the latest patch to the outdated software as soon as possible. The vulnerabilities found on the HP switches consist of TLS/SSL certificate vulnerabilities and deal mainly with using outdated encryption suites. Though outdated/self-signed certificates on internal devices are not as high risk as the same on external facing devices, proper, up-to-date SSL certificates should be installed to meet best practice.

Additionally, switches were found to be running variations of 3 versions of firmware; these switches should be updated to the newest firmware supported by the vendor.

Results

We have included supplemental material to this report consisting of the Nessus scan results and Pentest report.

Scan Results - The scan results provide granular detail of each vulnerability, which are categorized by their severity: critical, high, medium, and low. An expanded definition of the known threat and solutions for remediating the vulnerability are also available.

Pentest Report – The Pentest Report provides a comprehensive analysis of the scan results.