

**No. 1(1)/Network-Misc/2023**  
**GOVERNMENT OF PAKISTAN**  
**MINISTRY OF SCIENCE AND TECHNOLOGY**  
\*\*\*\*\*

Islamabad, the 14<sup>th</sup> June, 2024

- |  |   |   |
|--|---|---|
| 1. The Chairman<br>PCSIR, <u>Islamabad</u>         | 2. The Chairman<br>PSF, <u>Islamabad</u>                | 3. The Chairman<br>PCST, <u>Islamabad</u>           |
| 4. The Chairman<br>CWHR, <u>Karachi</u>            | 5. The Chairman<br>PEC, <u>Islamabad</u>                | 6. The Rector<br>NUST, <u>Islamabad</u>             |
| 7. The Rector<br><u>NUTECH, Islamabad</u>          | 8. The Rector<br>COMSATS University<br><u>Islamabad</u> | 9. The Director General<br>NIE, <u>Islamabad</u>    |
| 10. The Director General<br>PNAC, <u>Islamabad</u> | 11. The Director General<br>PSQCA, <u>Karachi</u>       | 12. The Director General<br>PCRET, <u>Islamabad</u> |
| 13. The Director General<br>NIO, <u>Karachi</u>    | 14. The Director General<br>PHA, <u>Islamabad</u>       | 15. The Director General<br>NMIP, <u>Islamabad</u>  |
| 16. The Managing Director<br>STEDEC, <u>Lahore</u> |   |   |

**Subject: ANALYSIS REPORT PHISHING BASED ADVACNED PRESISTENT THREAT (APT) TARGETING BUREAU DIVISION's (IBD) OFFICERS (ADVISORY No. 08)**


Dear Sir,

Please find enclosed herewith Cabinet Division's letter No.1-5/2023/ 24(NTISB-II) dated: 09-05-2024 on the subject cited which is self-explanatory.

2. In view of the above, all concerned are requested for strict compliance and to take necessary protective measures at their end.

**Encl. as above**

Yours faithfully

  
(Abdul Moiz Waqar Khan)  
Network Supervisor  
Ph: 9216407

Copy for information to:

- APS to JEA, MoST



GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT  
CABINET DIVISION  
(NTISB)

F. No. 1-5/2003/24(NTISB-II)

Islamabad, the 9<sup>th</sup> May, 2024

Subject:- Analysis Report Phishing Based Advanced Persistent Threat (APT) Targeting Intelligence Bureau Division's (IBD) Officers (Advisory No. 08)

Recently, an Advanced Persistence Threat (APT) campaign has been observed targeting the Intelligence Bureau Division's (IBD) officers through phishing attacks. The attackers aimed to steal sensitive information from the computers under the use of IB officers. On 30-04-2024, IBD HQ identified a suspicious file named "2nd NAP Coordination Committee Meeting.rar" file through WhatsApp message. The attacker impersonated as a NACTA official and sent messages to IBD HQ's Senior Officer from WhatsApp number 03557876530.

2. Upon inquiry, the CMO Special Communication Organization (SCO) informed that the WhatsApp number does not exist in their record. Few details are attached as Annex-A.

3. Identified Malware Capabilities. There were two malicious zip files identified as under:

- a. Minutes of second NAP CCM.pdf.chm
- b. SearchApp.exe.

4. Second file is the windows hidden executable file created to execute on opening of the first file a malicious code on the target Operating system. Initial analysis suggests the presence of information-stealing malware. This type of malware can:

- a. Capture keystrokes, including login credentials and sensitive documents.
- b. Take screenshots of user activity.
- c. Exfiltrates files from the compromised devices through secure encrypted channel and Command & Control Server.
- d. Malware contacts the Linux based Command-and-Control server hosted by M247 Europe SRL to covert data transfer through encrypted (SSL) channels. Details are as under:

(1) **IP Address:** 162.252.175.170 Ports: 22, 3389, 443 (used for malware communication).

(2) **Company:** M247 Europe SRL is a hosting and cloud services provider.

N/S MOST

Discussed with JFA.  
Circulate for necessary  
action/compliance

12/6/24

DEA/II

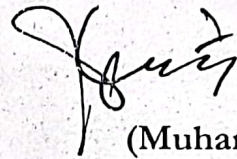
12-6-24



5. **Potential Impacts.** The above attack poses a significant threat as attacker aimed to steal the sensitive data from the computers used by the Senior Government Officers.

6. **Recommendations.** All Government Officials are advised to adopt cautious approach and do not use WhatsApp for official correspondence specially sharing of official documents. Official documents received on WhatsApp as well as on email, be double checked from sender for authenticity.

7. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.



(Muhammad Usman Tariq)  
Assistant Secretary-II (NTISB)  
Ph# 051-9204560

**All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments**

**Copy to:**

1. Principal Secretary to the PM, Prime Minister's Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad




## WhatsApp Profile of the Attacker



+92 355 7876530

~Md. Humza~


Not a contact · No common groups

 Safety Tools

Block

Add




## Malware Analysis


 **SearchApp.exe**


**Analyzed on:** 04/30/2024 06:37:00 (UTC)

**Environment:** Windows 10 64 bit

**Threat Score:** 100/100

**Indicators:**   

**Network:** 



# Detection using Machine Learning and Static Analysis Results Indicators of Compromise

## Malicious Indicators

## External Systems

Sample detected by CrowdStrike Static Analysis and ML with relatively high confidence

details CrowdStrike Static Analysis and ML (QuickScan) yielded detection: win/malicious\_confidence\_100% (W)

source External System

relevance 10/10

## Contacted Hosts

View 1 of 1 contacts in this category

### IP Address

162.252.175.170

### Port/Protocol

443  
TCP

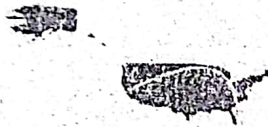
### Associated Process

searchapp.exe  
PID: 104

### Details

 United States

## Contacted Countries





GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT  
CABINET DIVISION  
(NTISB)

F. No. 1-5/2003/24(NTISB-II)

Islamabad, the 10 June, 2024

Subject: Advisory – Cyber Security Threats and Privacy Concerns – Cautious Usage of AI Driven ChatBots (Advisory No. 09)

Context. OpenAI launched ChatGPT in November, 2022; gathering a widespread usage and audience. With this, issues regarding positive and negative aspects concerning cyber security and privacy concerns have come to the forefront. Consequently, an advisory on Chat GPT with emphasis on its cyber security challenges/aspects was shared on 19<sup>th</sup> June, 2023 and 11<sup>th</sup> July, 2023. Off late, ChatGPT and other similar models (Bard, CoPilot, MyAi etc.) are integrated in major Social Media platforms, Web Browsers and Smart Phones. Given the exponential rise in usage of AI Driven ChatBots, the safety measures and cautious use of ChatGPT/ChatBots at organizational and individual level are illustrated in the ensuing paras.

2. Growing Trend – AI Driven ChatBots. Globally, many organizations are integrating ChatGPT and other AI powered ChatBots/APIs into their operational flow/information systems. ChatGPT accounts signify the importance of AI-powered tools along with the associated cyber risks as it allows users to store conversations. In case of breach, access of a user account may provide insight into proprietary information, area of interest/research, internal operational/business strategies, personal communications and software code etc.

3. Precautionary Measures

a. Users

- (1) ChatGPT/other AI-powered ChatBots and APIs must not be used by users handling extremely sensitive data. Masking of critical information may be utilized where absolutely essential.
- (2) Do not enter sensitive data which reveals own capability/held resources etc. into ChatBots. If essential, ensure to disable the chat saving feature from the platform's settings menu or manually delete those conversations as soon as possible.

- (3) Use a malware free/screened system for ChatBots. An infected system with information stealer malware may take screenshots or perform keylogging leading to a data leak.

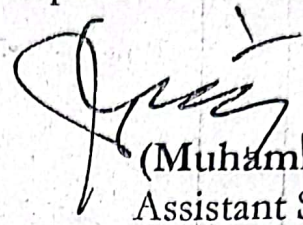
b. **Organizations.** Through best practices at organizations can ensure that ChatBots are used securely and the data is protected. It is also important to note that AI technology is constantly evolving. The key to protection may be that organizations must stay up-to-date with the latest security trends. Few best practices (but not limited to) are as follows:

- (1) **Dedicated Online PC for ChatBot Usage.** To ensure data protection and countering pilferage of sensitive official data, separate online PC with no private/official data be used for using AI driven ChatBots.
- (2) **Conduct Risk Assessment.** Comprehensive risk assessment of AI Driven ChatBots be performed to identify any potential/exploitable vulnerabilities. This will help organizations to develop a plan to mitigate risks and ensure that their data is protected.
- (3) **Mechanism to Monitor Access.** It is important to monitor that who has access to ChatBots. A mechanism be ensured that access is granted only to authorize individuals. This can be achieved by implementing strong access controls and monitoring access logs.
- (4) **Implement Zero-Trust Security.** Zero trust security (an approach that assumes that every user and device on a network is a potential threat) be adopted. This means that access to resources should be granted only on need-to-know basis followed by strong authentication mechanism.
- (5) **Use Secure Channels.** To prevent unauthorized access to AI Driven ChatBots, secure channels be adopted to communicate. It includes using encrypted communication channels and secure APIs.



- (6) Train the Employees. Employees be trained on cautious usage of ChatBots and the potential risks associated with its use. It, must be ensured that the employees do not share sensitive data with chatbot and are aware of the potential for social engineering/malicious attacks.

4. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.

  
(Muhammad Usman Tariq)  
Assistant Secretary-II (NTISB)  
Ph# 051-9204560

All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Copy to:

1. Principal Secretary to the PM, Prime Minister's Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad



GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT  
CABINET DIVISION  
(NTISB)

F. No. 1-5/2003/24(NTISB-II)

Islamabad, the 10 June, 2024

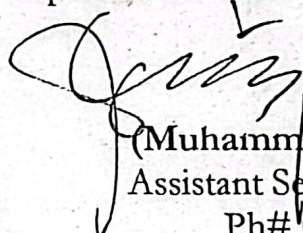
Subject: Cyber Security Advisory - VMWare Workstation & Fusion Patch Update (Advisory No. 10)

Introduction. Multiple vulnerabilities affecting VMWare Workstation & Fusion have been identified and addressed through upgrades by VMWare.

2. CVE Details. CVE-2024-22267 (a use-free vulnerability) allows an attacker with local administrative privileges to execute arbitrary code on the host. CVE-2024-22268 (a heap buffer-overflow vulnerability) which can potentially lead to a denial of service condition. CVE-2024-22269 & CVE-2024-22270 (information disclosure vulnerabilities) allows attacker to access privileged data with local administrative privileges.

3. Recommendations. Users are advised to apply security patches by updating VMWare Workstation to version 17.5.2 or later and Fusion to version 13.5.2 or later.

4. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.



(Muhammad Usman Tariq)  
Assistant Secretary-II (NTISB)  
Ph# 051-9204560

All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Copy to:

1. Principal Secretary to the PM, Prime Minister's Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad



GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT  
CABINET DIVISION  
(NTISB)

F. No. 1-5/2003/24(NTISB-II)

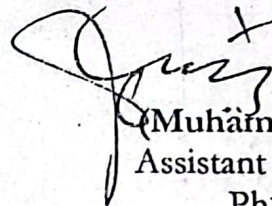
Islamabad, the 10 June, 2024

Subject: Cyber Security Advisory – Google Chrome Release Security Update (Advisory No. 11)

Introduction. Google has released an emergency security update for its Chrome Browser to address critical vulnerabilities. The update, patches CVE-2024-4671, which could allow remote attacker to escape the browser's sandbox via specially crafted webpages. Another patched vulnerability, CVE-2024-4761, involves an out-of-bound write in Google's V8 JavaScript engine, also exploitable through crafted webpages. Keeping Chrome updated is crucial to mitigate these security risks effectively.

2. Recommendations. To safeguard against Chrome vulnerabilities, users shall ensure that their Chrome browser is updated to version 124.0.6367.207 or later by navigating to Setting>About Chrome and relaunching the browser if an update is available.

3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.



(Muhammad Usman Tariq)  
Assistant Secretary-II (NTISB)  
Ph# 051-9204560

All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Copy to:

1. Principal Secretary to the PM, Prime Minister's Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad