CERT & NIC GUIDELINES

Hari Haran
NIC-CERT

AGENDA

1 Key Security Incidents

2 Mobile Security

3 Server & App Security

4 Best Practices

Key Security Incidents

Cyber Security Guidelines

RESTRICTED

Government of India
Cyber Security Do's & Don'ts

Cyber Security Guidelines for
Government Employees

MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY

A-Block, CGO Complex
New Delhi – 110003
Website: https://www.nic.in/

Cyber Security Guidelines – Access Restrictions

RESTRICTED

Government of India

Cyber Security Do's & Don'ts

DISTRIBUTION LIST:

The following persons hold copies of the documents; all amendments and updates to the document must be distributed to the distribution list.

S.No.	Name	Location	Document type
1	Government Ministries and Departments	Across India	Soft copy

CONFIDENTIAL:
This document contains restricted information pertaining to the National Informatics Centre. The access level for the document is specified above. The addressee should honor this access right by preventing intentional or accidental access outside the access scope.

DISCLAIMER:
This document is solely for the information of the government employees and outsourced/contractual resources and it should not be used, circulated, quoted or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent of NIC/MeitY.

Cyber Security Guidelines – contd…

{* SECURITY *}

Indian government issues confidential infosec guidance to staff – who leak it

Bans VPNs, Dropbox, and more

Simon Sharwood, APAC Editor

Mon 20 Jun 2022 // 03:32 UTC

India's government last week issued confidential information security guidelines that calls on the 30 million plus workers it employs to adopt better work practices – and as if to prove a point, the document quickly leaked on a government website.

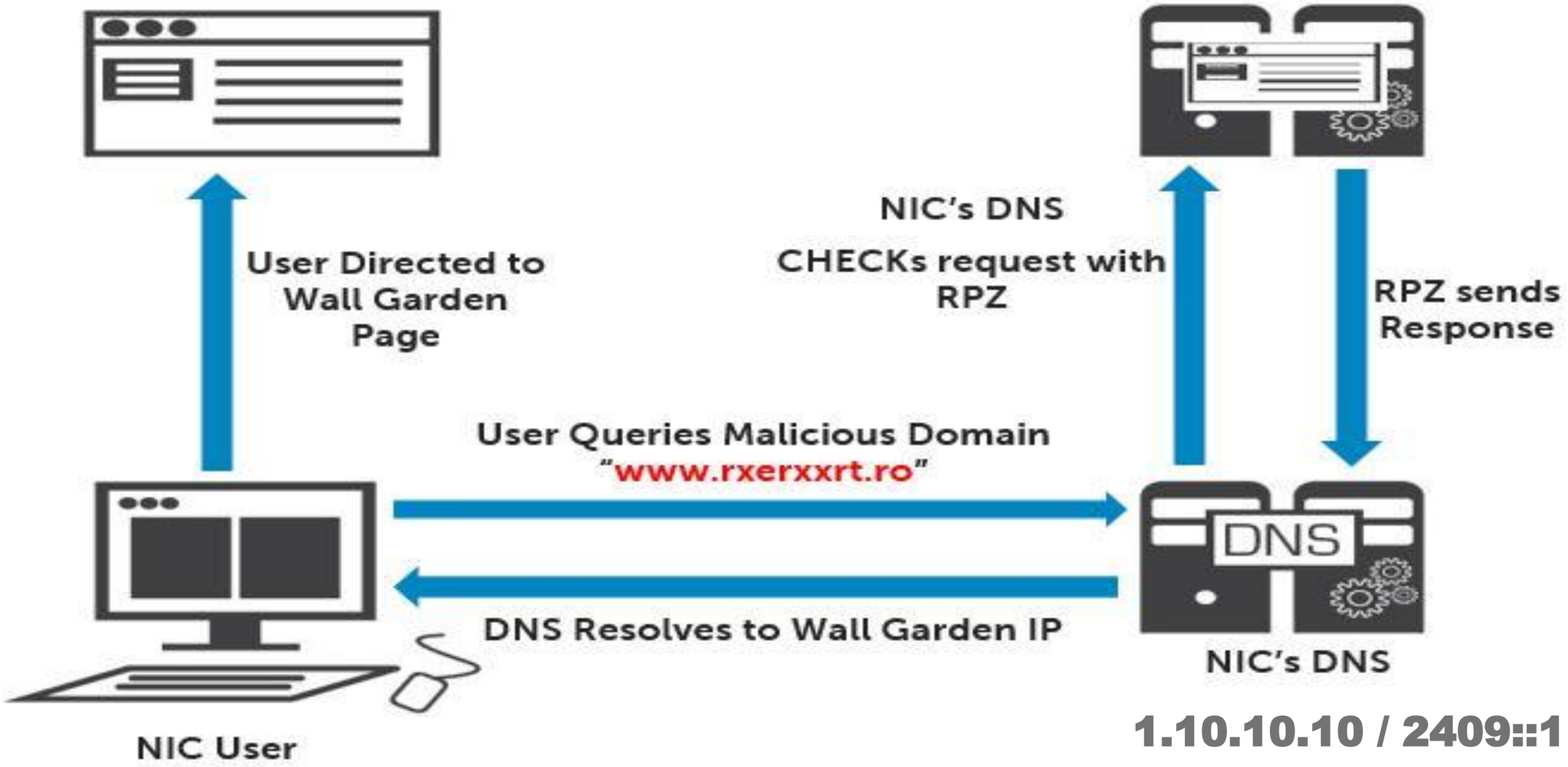
The document, and the measures it contains, suggest infosec could be somewhat loose across India's government sector.

"The increasing adoption and use of ICT has increased the attack surface and threat perception to government, due to lack of proper cyber security practices followed on the ground," the document opens.

"In order to sensitize government employees and contractual/outsourced resources and build awareness amongst them on what to do and what not to do from a cyber security perspective, these guidelines have been compiled."

Ironically, the document proves why it's needed. Despite being marked

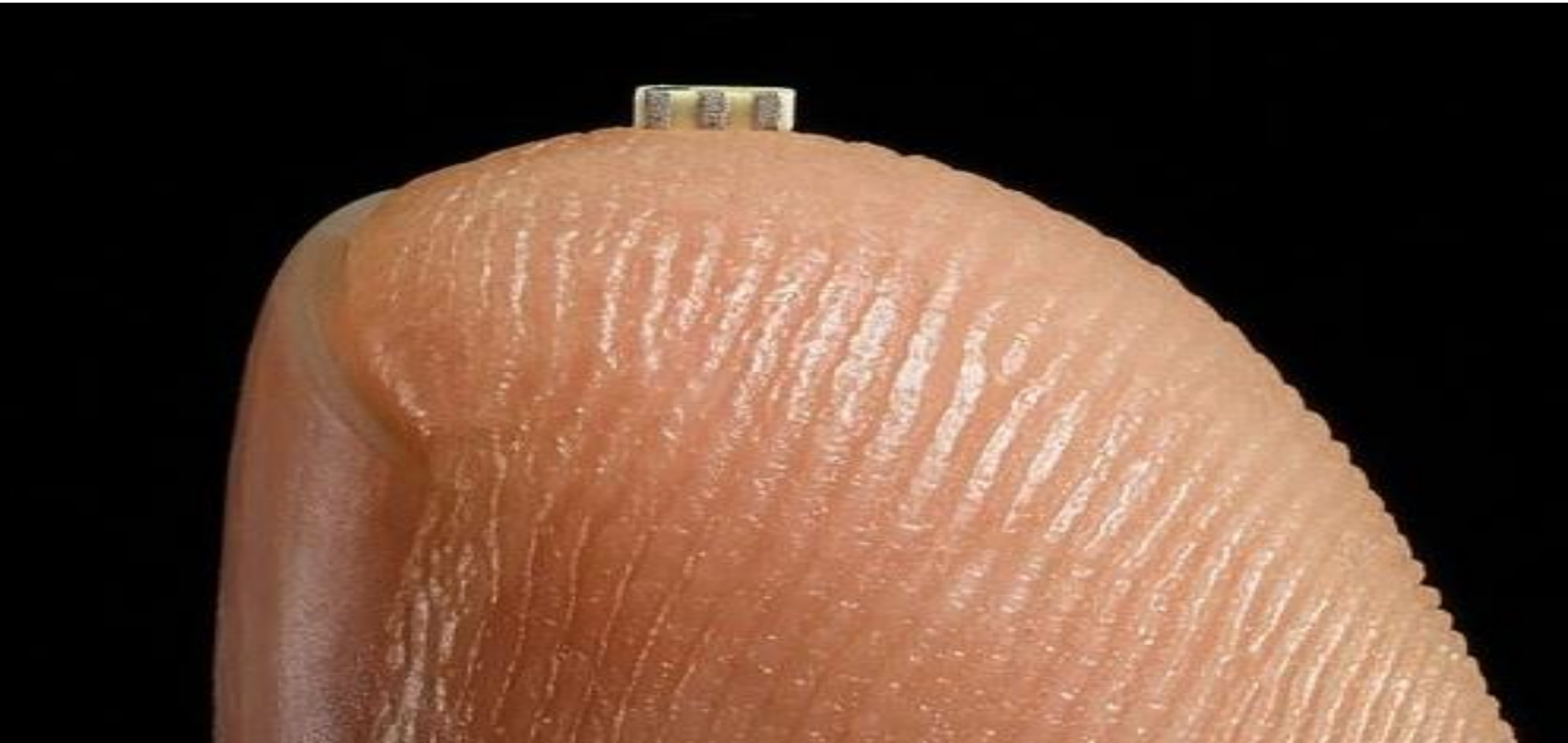
Use DNS – 1.10.10.10 / 2409::1



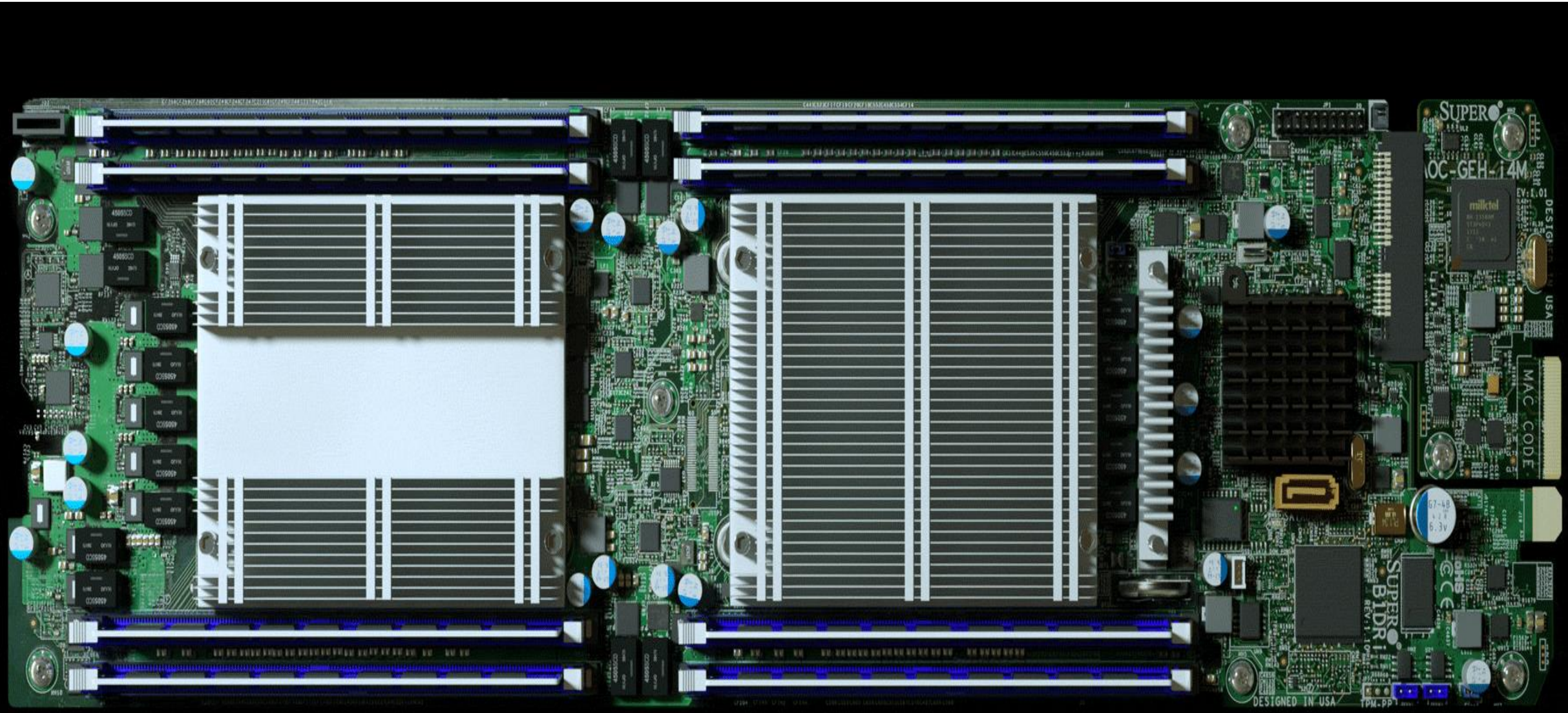
AIIMS - INCIDENT

Supply Chain Security

What is this?



Server Mother Board with Implant Chip

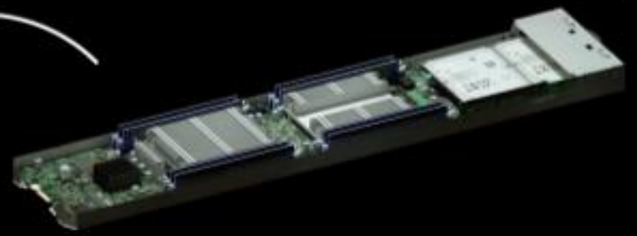


How the Hack was alleged to be Done

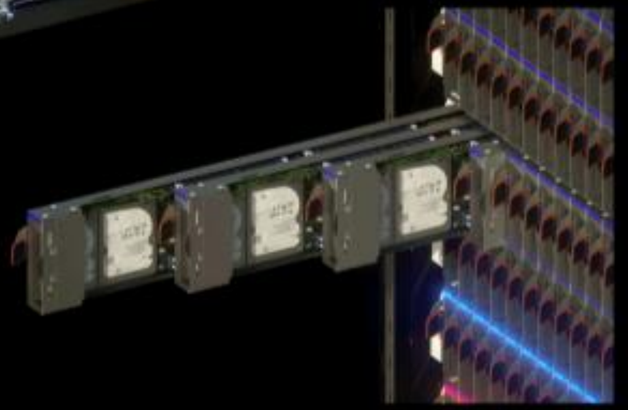
❶ A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip. Some of the chips were built to look like signal conditioning couplers, and they incorporated memory, networking capability, and sufficient processing power for an attack.

❷ The microchips were inserted at Chinese factories that supplied Supermicro, one of the world's biggest sellers of server motherboards.

❸ The compromised motherboards were built into servers assembled by Supermicro.



❹ The sabotaged servers made their way inside data centers operated by dozens of companies.



❺ When a server was installed and switched on, the microchip altered the operating system's core so it could accept modifications. The chip could also contact computers controlled by the attackers in search of further instructions and code.

Supply Chain Risk Mitigation

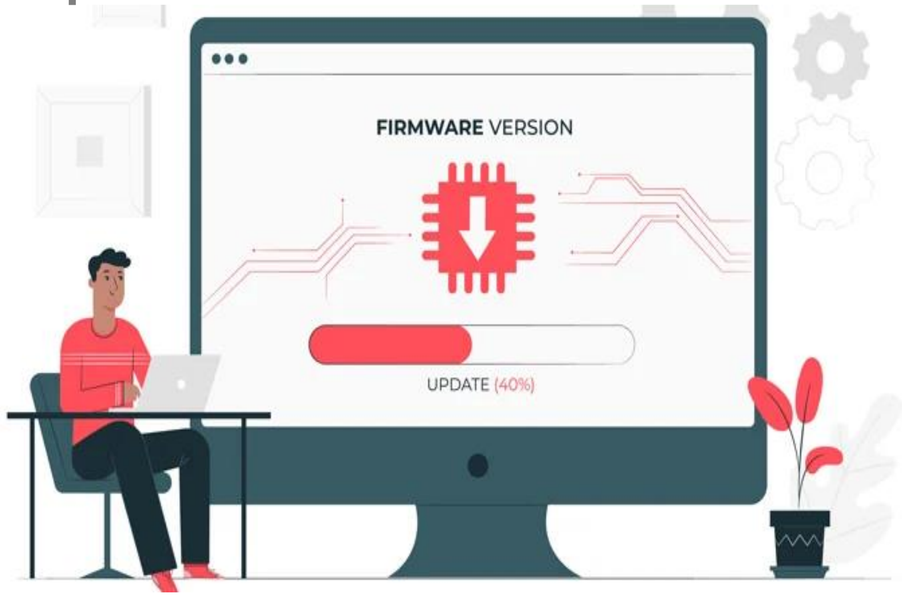
- Avoid Sharing Project name, Model & Specs of existing devices, in public RFP/Tenders

- Sign NDA with bidders, before sharing details

- Share necessary details in printed document with unique watermarking for each document

Supply Chain Risk Mitigation

- Update Firmware & BIOS regularly
- Obtain the hash of patch/updates from OEM and verify the integrity of the downloaded patch/update
- Block All Outbound communication from Data Centre, allow communications on a need basis

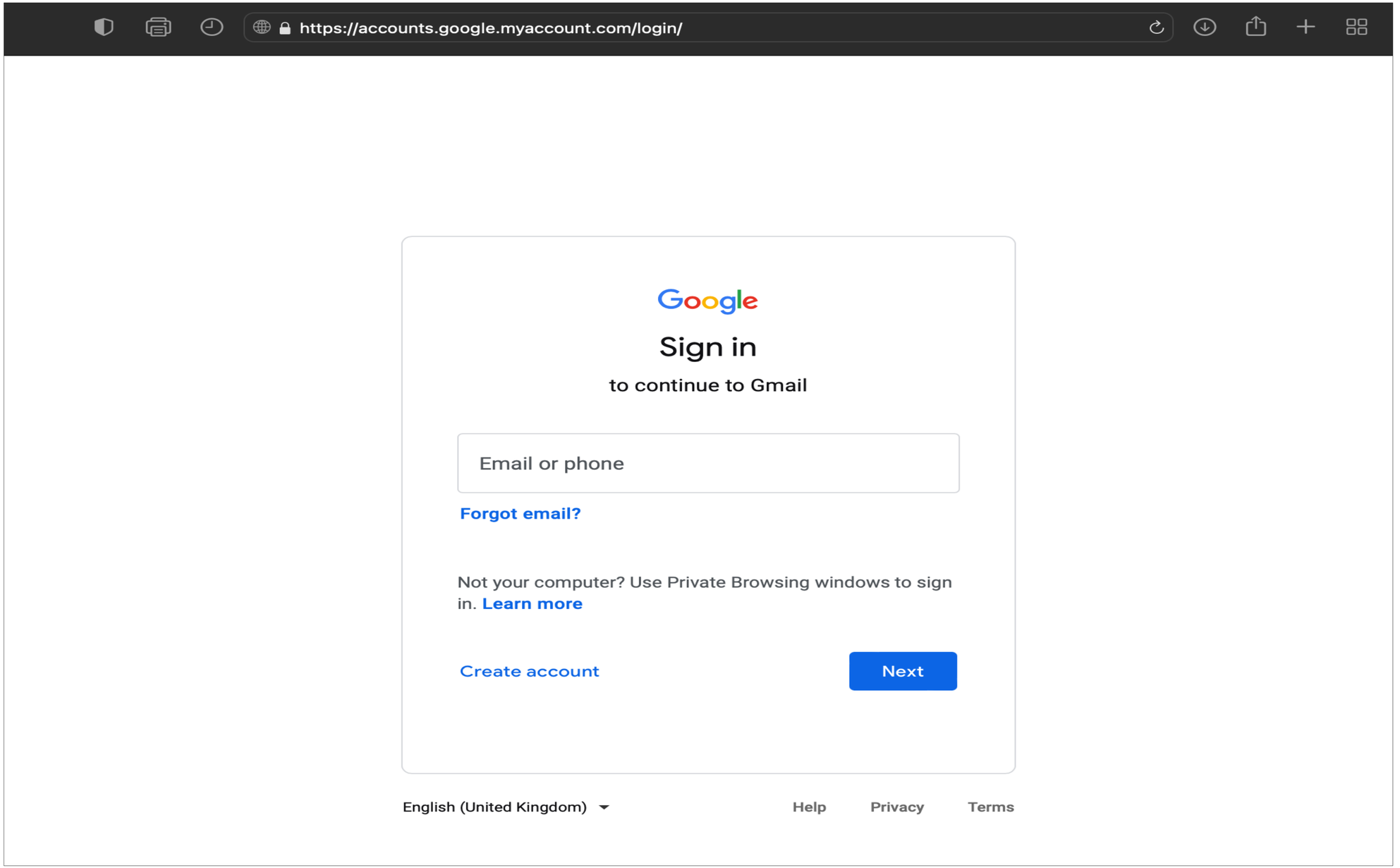


Phishing Attacks

Phishing Mail

Hi,
You have consumed 100% of your google free storage. You will not be able to send/receive emails and cannot store any additional data in your google account. To continue using the google account, please delete your files or you can purchase additional storage space. Click here to continue
https://accounts.google.myaccount.com/login

Phishing Mail



Phishing Mail : What you can Do?

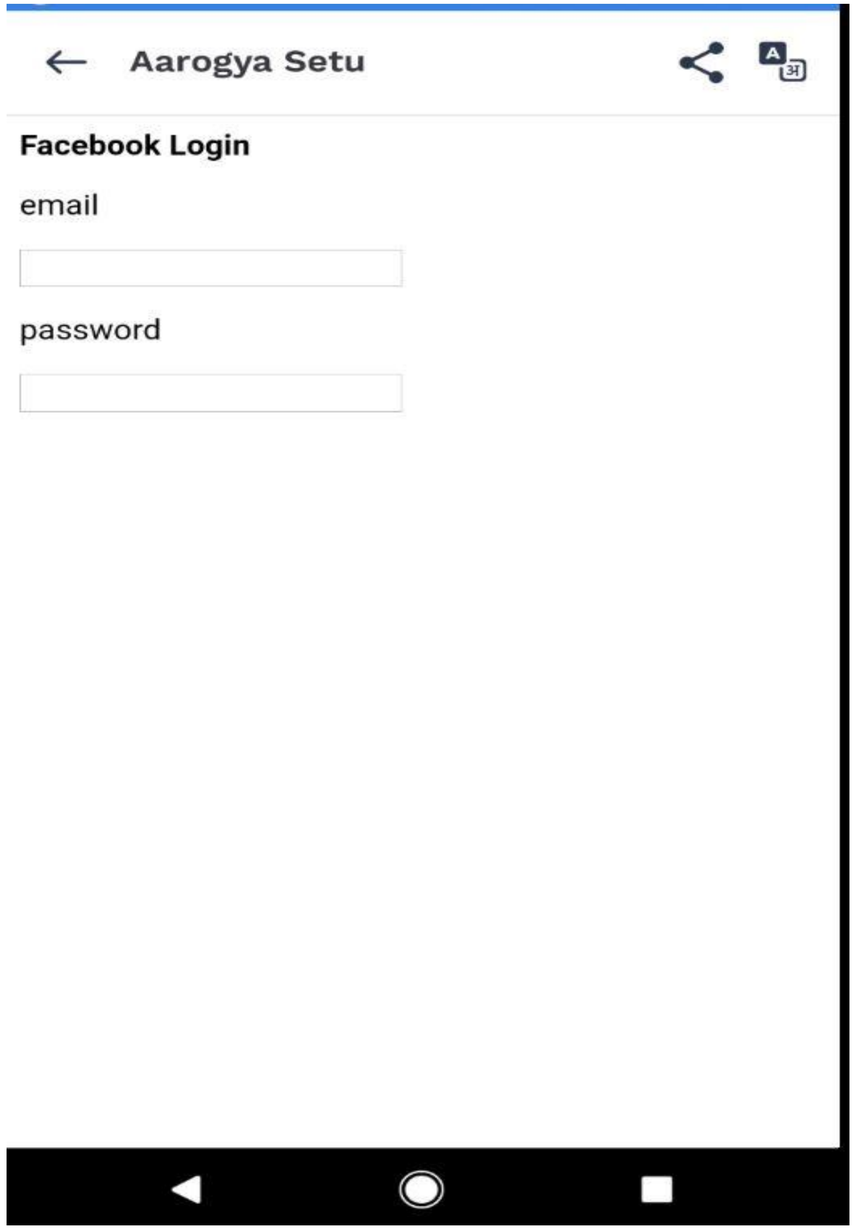
1. Report Phishing Incidents :
   incident@cert-in.org.in / incident@nic.in

2. Don’t open attachments and Don’t click on the links and Don’t Forward Phishing Mails to other users

3. Don’t upload Phishing mail samples or attachments to external sites like Virustotal.com

Mobile Security

Fake Aarogyasetu App - Login



Aarogya Setu - Fake App

23 engines detected this file

4b59f9e400691d5d4d4573235aa22abbe9440373f3ffea433bb359f0587ec109

Aarogya_Setu.apk

android apk

3.05 MB
Size

2020-04-27 09:06:09 UTC
6 hours ago

APK

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

AegisLab	Trojan.AndroidOS.Masplot.C!c	AhnLab-V3	PUP/Android.Metasploit.373726
Alibaba	TrojanDownloader:Android/Masplot.8590...	Avast	Android:Metasploit-P [PUP]
Avast-Mobile	APK:RepSandbox [Trj]	AVG	Android:Metasploit-P [PUP]
Avira (no cloud)	ANDROID/Dldr.Agent.PAE.Gen	CAT-QuickHeal	Android.Agent.ACZ
DrWeb	Android.RemoteCode.67	ESET-NOD32	A Variant Of Android/TrojanDownloader....
F-Secure	Malware.ANDROID/Dldr.Agent.BI.Gen	Ikarus	Trojan-Downloader.AndroidOS.Agent
K7GW	Trojan (0054e2a01)	Kaspersky	HEUR:Trojan-Downloader.AndroidOS.M...
MAX	Malware (ai Score=99)	McAfee	Artemis!2B67566ECDB6
Microsoft	Trojan:Win32/Bluteal!rfn	Qihoo-360	Trojan.Android.Gen
Symantec	Trojan.Gen.MBT	Symantec Mobile Insight	Other:Android.Reputation.1

Phone Permissions Required By Fake App

- android.permission.ACCESS_COARSE_LOCATION
- android.permission.ACCESS_FINE_LOCATION
- android.permission.BLUETOOTH
- android.permission.BLUETOOTH_ADMIN
- android.permission.CALL_PHONE
- android.permission.CAMERA
- android.permission.CHANGE_WIFI_STATE
- android.permission.INTERNET
- android.permission.READ_CALL_LOG
- android.permission.READ_CONTACTS
- android.permission.READ_PHONE_STATE
- android.permission.READ_SMS
- android.permission.RECEIVE_SMS
- android.permission.RECORD_AUDIO
- android.permission.SEND_SMS
- android.permission.WRITE_CALL_LOG
- android.permission.WRITE_CONTACTS
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.ACCESS_BACKGROUND_LOCATION
- android.permission.ACCESS_NETWORK_STATE
- android.permission.ACCESS_WIFI_STATE
- android.permission.FOREGROUND_SERVICE
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.SET_WALLPAPER
- android.permission.WAKE_LOCK
- android.permission.WRITE_SETTINGS
- com.google.android.c2dm.permission.RECEIVE
- com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Mobile Platform Risks

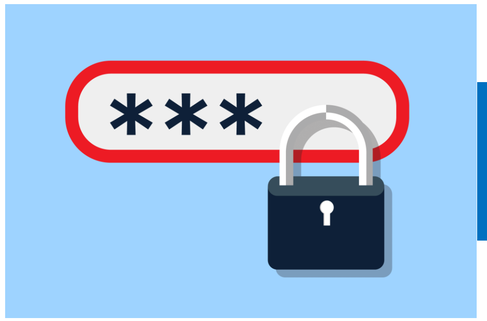
Device Risks

Rooted / Jailbroken Devices
Outdated OS Security
Vulnerabilities
Malware

App Risks

Insecure App Coding
App Hacking / Reverse Engineering
Cryptographic Key Theft

Basic Mobile Hygiene



Use strong and difficult-to-guess passwords for your computer and mobile phone.

Use the latest versions of operating systems, applications and browsers. Don’t jailbreak or root mobile devices.

Install and update software applications promptly. Do not download files from untrusted sources. Download applications from official application store only.

Use secure peripheral devices and disable any network functionality when not in use (e.g. Wi-Fi, Bluetooth, NFC etc.). Avoid connecting to Public Wifi Hotspots

Server & App Security

Security Measures @ Server

- Periodic Security Audit of App and Infra
- Geofence Applications/Websites
- HIPS for host level DPI, Virtual Patching & Integrity Monitoring
- Web Application Firewall for Application Layer Inspection
- Offload SSL/TLS Certificates before Network IPS
- Host Level Firewall for lateral movement restriction
- Security Audit of Platform and Application
- Log Analysis & Offline/Offsite Backup

Securing Operating System Platform

Do You Know ?

83% of all Critical Vulnerabilities published by Microsoft during the last 5 years can be mitigated by using a non-admin User Account

- 858 Microsoft Product Vulnerabilities were discovered in 2019
- Removing admin rights would mitigate 77% of all critical Microsoft vulnerabilities published in 2019
- 80% of Critical vulnerabilities in Windows Servers could be mitigated by using a non-admin user account.
- 100% of critical vulnerabilities in Internet Explorer could be mitigated by using a non-admin User account
- 80% of Critical Vulnerabilities in Windows 7, 8.1 and 10 could be mitigated by using a non-admin account

Keep your Operating System and Antivirus Updated with latest Patches/Updates

Create a non-admin account in your OS/ System and Use it for day to day activities

Don't use any Pirated Softwares or Cracks or Keygens.

Disable Powershell and Remote Desktop

Report Security Incident to NIC-CERT :

011-22902400 incident@nic-cert.nic.in https://nic-cert.nic.in

Cyber Hygiene For Govt. Staffs

NIC CERT
Observe - Detect - Respond

Download Mobile Apps only from the official Appstore (ex: Google Playstore, Apple App Store). ` Downloading less popular Apps may be avoided

Don't root or jailbreak your mobile phone

Don't Use Pirated Softwares

Use NIC Provided Antivirus Client and ensure that it is updated regularly

Keep Your Operating System, softwares and browsers Updated with the Latest Updates.

Avoid using remote admin tools like anydesk, ammy admin & team viewer

Take regular backup of your Data

Ensure NIC's DNS '164.100.3.1' is configured as default DNS in your system's network settings

Don't Use/Register Government Email Address (@gov.in, @nic.in) in any 3rd party (non-Govt) website or App

Don't Click on any links sent by Unknown Senders

Don't Use the same Password in multiple sites

Use Multi-Factor Authentication (If available) Never share your passwords and OTPs with anyone

Use Complex Passwords with min. 8 letters - combination of Upper case, Lower case, numbers and special characters.

Change Passwords regularly and Don't save the passwords in browser

Before clicking on a Shortened URLs (ex: **http://bit.ly/br6432**), use an url expander service (ex : **https://urlcheck.nic.in**) to check the original url

Check for https with green padlock on sites where you login or carry out financial transactions

Report Security Incident to NIC-CERT : incident@nic-cert.nic.in / +91-011-2290-2400

एनआईसी National Informatics Centre

NIC CERT
Observe - Detect - Respond

www.nic-cert.nic.in
incident@nic.in
+91-22902400

THANK YOU