INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC

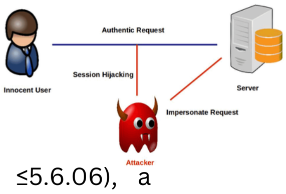
DOI No. 10.5281/zenodo.15515683

APRIL 2025

CYBER BULLETIN

Cyber Surge & Warfare

BigAnt Hijack 1.



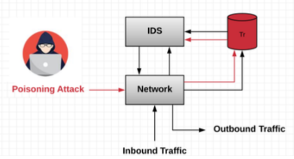
SESSION EXPLOITATION

TARGET: BigAntSoft's BigAnt Server (v ≤5.6.06), a Windows-based enterprise chat and collaboration platform.

IMPACT: Attackers hijack sessions, access the cloud drive add-in and achieve full RCE by uploading malicious PHP files.

MITIGATION: Update the software promptly, disable unused signup features, restrict access to system tools and use filters to block harmful uploads.

New Mexico School Hack 3.



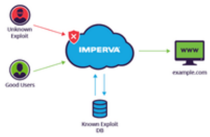
POWERSHELL INTRUSION

TARGET: Administrative networks of New Mexico educational institutions (student systems unaffected).

IMPACT: Disrupted admin operations, risk of staff data theft and hidden malware enabling deeper system access.

MITIGATION: Use MFA for admin accounts, separate admin and student networks and deploy real-time endpoint protection.

Morocco Data Breach 5.



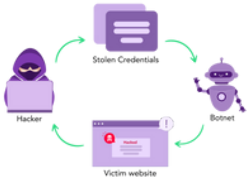
EXPLOITING VULNERABILITIES

TARGET: Morocco's National Social Security Fund (CNSS) managing data for millions of citizens.

IMPACT: Over 54,000 files leaked impacting 2 million individuals. The breach is linked to geopolitical tensions and cross-border risks.

MITIGATION: Update software regularly, watch out for cyber threats linked to international conflicts and keep affected people informed during any security breach.

IoT Siege 2.



Credential Stuffing

TARGET: Telecom providers and online gaming servers, mainly via compromised security cameras and NVRs.

IMPACT: Over 86,000 IoT devices infected, enabling large-scale DDoS attacks that disrupt networks and services.

MITIGATION: Update firmware, use strong passwords, disable unused remote access and isolate IoT devices from core networks.

Digital Warfare 4.

Website
Administrator
Network
CMS
Content Management System
Content
PDF-HTML
Data
Open-Source
Domain

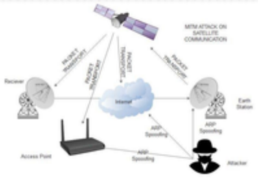
CMS EXPLOITATION

TARGET: India's critical sectors, including education, defense, banking, and communication, following the Pahalgam terror attack.

IMPACT: Over 1 million attempted breaches, website defacement and sensitive data released on the dark web

MITIGATION: Strengthen vulnerability management, conduct penetration tests and enhance data encryption and monitoring.

Iranian Ship Attack 6.



SATELLITE DISRUPTION

TARGET: Iran's key maritime firms, NITC and IRISL, vital to the nation's oil exports and logistics.

IMPACT: 116 ships communications cut, disrupting Iran's oil trade and regional logistics. Recovery may take weeks revealing vulnerabilities in satellite systems.

MITIGATION: Upgrade satellite systems, create backup communication plans and boost cybersecurity through collaboration.

INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC

DOI No. 10.5281/zenodo.15515683
APRIL 2025

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

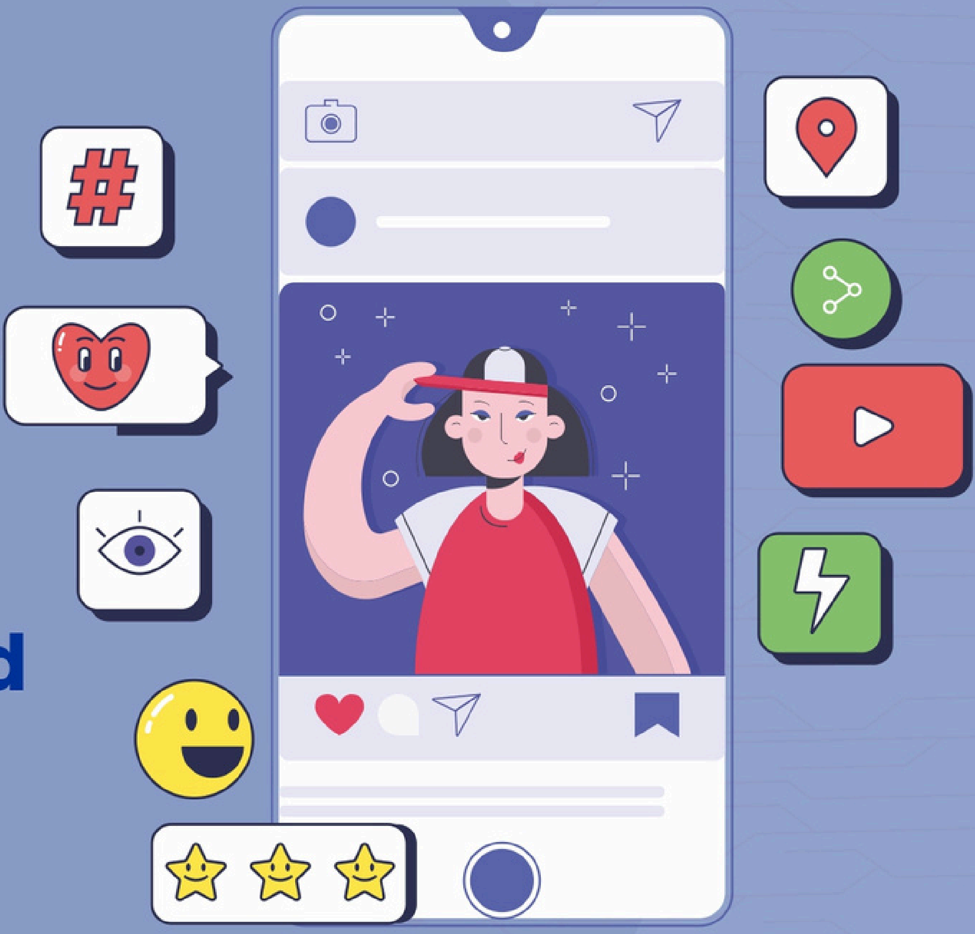
ISEA
www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

CYBER SECURITY
POSTER OF THE DAY

Enjoy social media responsibly

Keep personal details private and enable privacy settings



#Sat Social Stay Safe

Supported by

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India
Power To Empower

myGov
मेरी सरकार

Indian Cyber Crime Coordination Centre

सी डैक
CDAC

CYBER SAKCHHARTA ABHIYAN
UNDER THE AEGIS OF
CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION

FACULTY COORDINATORS
MR. SHUBHAM KUMAR | MR. FAIZAN MAHMOOD | MR. MOHD TALHA
STUDENTS COORDINATORS
MOHAMMAD FARHAN | SIDRA SIDDIQUI | ELMA SHARIQ
AREEBA KHAN | ANAMTA ANSARI

Prof.(Dr.) MOHAMMAD FAISAL
Head, Department of Computer Application