GATEWAY INSTITUTE OF
ENGINEERING & TECHNOLOGY
Delhi-NCR, Sonipat
Approved by AICTE, New Delhi & Affiliated to DCRUST, Murthal

CYBER
BULLETIN
VOLUME-1

CYBER BULLETIN

CYBER HEISTS

CRYPTOCURRENCY 1.

EXCHANGE HEIST

TARGET: Cryptocurrency exchanges and digital wallets.

IMPACT: Theft of over $1 billion in cryptocurrencies, loss of investor confidence, and market instability.

MITIGATION: Implement multi-signature wallets and cold storage, enhance security protocols, and conduct regular security audits.

SUPPLY CHAIN ATTACK 2.

COMPROMISED SOFTWARE UPDATES

TARGET: Software supply chain and third-party vendors.

IMPACT: Infiltration of malicious code into trusted software, widespread impact on users, costly mitigation efforts.

MITIGATION: Vet third-party vendors carefully, use code-signing certificates, implement robust monitoring and response strategies for supply chain security.

CLOUD STORAGE BREACH 3.

DATA LEAKS FROM THE CLOUD

TARGET: Cloud storage platforms and services.

IMPACT: Exposure of sensitive corporate data, financial losses, regulatory penalties.

MITIGATION: Encrypt data before uploading, implement strict access controls, conduct regular security audits of cloud providers.

CORPORATE ESPIONAGE 4.

INDUSTRIAL SECRETS STOLEN

TARGET: Home automation systems

IMPACT: Unauthorized voice command execution. Data interception through network vulnerabilities.

MITIGATION: Enable voice recognition features to ensure commands are from authorized users. Regularly update the speaker's firmware. Secure the home network with strong passwords and encryption.

IOT DEVICE HIJACKING 5.

SMART HOMES UNDER ATTACK

TARGET: Internet of Things (IoT) devices, including smart home systems.

IMPACT: Unauthorized access to personal data, potential physical security risks, disruption of connected services.

MITIGATION: Regularly update device firmware, change default passwords, segment IoT devices from main network.

BANKING TROJAN INVASION 6.

FINANCIAL INSTITUTIONS

TARGET: Online banking platforms and mobile banking apps.

IMPACT: Unauthorized access to customer accounts, fraudulent transactions, reputational damage.

MITIGATION: Deploy advanced anti-malware solutions, implement multi-factor authentication, educate customers on phishing attacks.

GATEWAY INSTITUTE OF
ENGINEERING & TECHNOLOGY
Delhi-NCR, Sonipat
Approved by AICTE, New Delhi & Affiliated to DCRUST, Murthal

CYBER
BULLETIN
VOLUME-1

WHILE SMALL IN SIZE, USB DEVICES CARRY A HUGE RISK

USB malware is more advanced than ever. Don't get bitten—only use approved, trusted, and clean devices.

SEL SCHWEITZER ENGINEERING LABORATORIES

For information about SEL cybersecurity solutions or copies of this poster, visit **selinc.com/cybersecurity**.
© 2018 by Schweitzer Engineering Laboratories, Inc. • LM00348-01 • 20180223

CYBER SAKCHHARTA ABHIYAN
UNDER THE AEGIS OF
CENTRE OF EXCELLENCE
ON CYBER SECURITY & NETWORKING
DEPARTMENT OF COMPUTER APPLICATION

Faculty Coordinator

Ms. Aruna Kapoor
Assistant Professor, Dept. of Computer Applications

Mr. Yogesh Khokhar
Head - IT Services