MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

November 2021

- US convenes Counter Ransomware conference
- Cyber attack takes Iranian centralised fuel distribution system offline
- Microsoft releases 2021 Digital Defence Report
- US issues new rules for software exports
- Cybersecurity guidelines released for Power sector

US convenes Counter Ransomware conference

A virtual Counter-Ransomware Initiative Meeting was convened by the United States National Security Council on the 13th and 14th of October, 2021. Thirty-two countries were invited to the meeting. A joint statement released at the conclusion of the Conference noted that the participating countries had taken note of the “need for urgent action, common priorities, and complementary efforts to reduce the risk of ransomware”. Efforts outlined included “improving network resilience to prevent incidents when possible and respond[ing] effectively when incidents do occur; addressing the abuse of financial mechanisms to launder ransom payments or conduct other activities that make ransomware profitable; and disrupting the ransomware ecosystem via law enforcement collaboration to investigate and prosecute ransomware actors, addressing safe havens for ransomware criminals, and continued diplomatic engagement.”[1]

Since taking office, the Biden Administration has undertaken a number of domestic and international initiatives on ransomware, including taking down ransomware infrastructure in third countries. This follows on the large number of ransomware attacks the US has faced in recent years—an estimate by the Treasury Department found that at least $ 400 million had been collected by way of ransomware in 2020 alone.[2]

Cyber attack takes Iranian centralised fuel distribution system offline

A cyberattack on the centralised fuel distribution system in Iran on 26th October took the entire system offline, making it impossible for motorists to buy subsidised fuel. 1,450 out of the total 4,300 fuel stations in the country were affected, according to the Iranian National Oil Products Distribution Company. Only about half of these had been reconnected to the network almost a week after the attack. Digital billboards on Iranian highways were also hacked into and displayed messages saying: "[Supreme Leader Ayatollah Ali] Khamenei, where is our fuel?"

Even though a group calling itself Predatory Sparrow claimed that it had carried out the hack, the Iranian leadership said state actors linked to the US and Israel were behind the attack, designed to foment unrest in Iran. The attacks were carried out on the anniversary of the 2019 fuel riots.[3] The same group had earlier claimed responsibility for an attack on the Iranian rail system in July, which caused public information boards at stations to incorrectly show trains as delayed or cancelled. The hackers had also, at that time, posted the phone number of Supreme Leader Ayatollah Ali Khamenei's office as the number to call for information.[4]

Microsoft releases 2021 Digital Defence Report

Microsoft released a comprehensive 134-page Digital Defence Report containing analysis from over 20 teams gleaned from 24 trillion daily security signals picked up by its millions of sensors across the globe. The report contains sections on nation state threats, supply chain, IoT and SCADA security, hybrid workforce security and disinformation as an emerging threat, particularly for enterprises.[5]

The report notes that Ransomware as a service has reached unprecedented levels of sophistication propelled by the high levels of profit for cyber-criminals. As IoT devices become ubiquitous in the home and the workplace, they represent a new point of attack through which attackers are gaining access to networks and devices. On the nation-state front, the report expects increased attacks on supply chain infrastructure as a means of penetrating software in the development stage, as end-point intrusion becomes more difficult to undertake and easier to identify.

The report concludes with actionable insights, noting that 98% of attacks can still be prevented by observing basic security hygiene practices.

US issues new rules for software exports

The United States issued new rules governing software exports on October 21 bringing it in line with the cybersecurity controls previously agreed to under the Wassenaar Arrangement in 2013.[6] The Commerce Department had earlier issued rules in 2015 which were withdrawn after negative feedback from the cybersecurity industry in the US and elsewhere for being too overly broad and detrimental to cross-border cybersecurity research.

The new rules, which are up for public comment till 6 December 2021, are more narrowly focused and also bring in new controls on certain cybersecurity items for National Security and Anti-terrorism reasons, while also creating exemptions allowing export to most countries. Countries that are barred from receiving exports include. Russia, China, Iran Cypress, Taiwan, and Singapore. Since the rules focus on specific cyber-intrusion and network surveillance equipment, software, and technology, it is expected that those most affected by the rules will be network infrastructure manufacturers, cybersecurity software and service providers, IT forensics firms, bug bounty programs, and vulnerability testing and research labs.[7] The announcement of the rules was couched as being part of the US government's fight against human rights violations.[8]

Cybersecurity guidelines released for Power sector

After setting up six sectoral CERTs for Thermal, Hydro, Transmission, Grid Operation, RE and Distribution, the Central Electrical Authority has now released guidelines to secure the electrical grid and associated infrastructure against cyber-attacks. The guidelines, in the form of 14 Articles and 3 Annexures, cover different aspects of cybersecurity. According to a statement from the power ministry, the guidelines put in place "mechanisms for security threat early warning, vulnerability management and response to security threats, securing remote operations and services, protection and resilience of critical information infrastructure, reducing cyber supply chain risks," whilst encouraging use of open standards, human resource development, effective public private partnerships and information sharing and cooperation.[9]

Notably, the guidelines mandate ICT-based procurement from identified 'trusted sources' and 'trusted products' or testing for malware and hardware backdoors before deployment for use in the power supply system network.[10] These guidelines have been put in place pending more comprehensive regulation from the Power Ministry. Amongst the other goals of these guidelines are promotion of cybersecurity research and development, and creation of a market for cyber testing infrastructure. There are an estimated 300-plus power utilities in India across the public and private sectors.

India File

- The second meeting of the India-UK Joint Working Group on Cyber

Capacity Building was held on 7 October 2021. The two delegations, headed by Shri Atul Malhari Gotsurve, Joint Secretary (Cyber Diplomacy), Ministry of External Affairs on the Indian side, and his counterpart, Mr. Andrew Dinsley, the Head of Cyber Programmes, Foreign, Commonwealth and Development Office (FCDO), on the British side, discussed various aspects of cooperation in the area of cyber capacity building. The meeting was held under the aegis of the India-UK Framework for Cyber Relationship, and in support of the Enhanced Cyber Security partnership agreed in the India-UK 2030 Roadmap. The first meeting of the JWG had been held on 05 March 2020 in New Delhi.

- The Fourth India-France Bilateral Cyber Dialogue was held on 13 October 2021. The two delegations, led respectively by Shri Atul Malhari Gotsurve, Joint Secretary (Cyber Diplomacy) from the Ministry of External Affairs, and Mr Henri Verider, Ambassador for Digital Affairs, Ministry of Europe, and Foreign Affairs of France, explored initiatives to further deepen cyber cooperation between the two countries. Experts present at the meeting agreed to work closely in the areas of cybersecurity, cybercrime, and capacity building.

- The Indian National Cyber Security Coordinator, Lt. Gen.Rakesh Pant, announced that the National Cybersecurity Strategy, in the works for the past two years, was currently before the Union Cabinet for approval, and would be out shortly. The Strategy, unlike the National Cybersecurity Policy of 2013, would be more broad-based and have finite timelines, budgets, and clear lines of responsibility for various entities. An overarching supervisory authority is also envisaged under the new strategy.

- The Indian Computer Emergency Response Team (CERT-In) has been authorized as CVE Numbering Authority (CNA) for vulnerabilities impacting all products designed, developed and manufactured in India. The CVE program, maintained by the Mitre Corporation was begun in 1999 to catalog and disseminate publicly known information-security vulnerabilities and exposures.

[1] "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting", at https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

[2] "Biden Sanctions Cryptocurrency Exchange over Ransomware Attacks", at https://www.reuters.com/business/finance/biden-sanctions-cryptocurrency-exchange-over-ransomware-attacks-2021-09-21/

[3] Iran blames foreign country for cyberattack on petrol stations at https://www.bbc.com/news/world-middle-east-59062907

[4] Iran says Israel, U.S. likely behind cyberattack on gas stations at https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/

[5] Microsoft's 2021 Digital Defense Report, at https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

[6] US Federal Register, Information Security Controls: Cybersecurity Items at https://www.federalregister.gov/documents/2021/10/21/2021-22774/information-security-controls-cybersecurity-items

[7] Being a White-Hat Hacker Just Got Tougher: U.S Commerce Department Issues New Cybersecurity Export Controls on Intrusion and Surveillance Tools at https://www.fenwick.com/insights/publications/being-a-white-hat-hacker-just-got-tougher-u-s-commerce-department-issues-new-cybersecurity-export-controls-on-intrusion-and-surveillance-tools

[8] US Department of Commerce, *Commerce Tightens Export Controls on Items Used in Surveillance of Private Citizens and other Malicious Cyber Activities*, at https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private

[9] PIB, Government releases guideline for the Cyber Security in Power Sector, at https://www.pib.gov.in/PressReleasePage.aspx?PRID=1761862

[10] Ministry of Power, *Cyber Security in Power Guidelines 2021* at https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf