NEWSLETTER

July 2018

National Critical Information Infrastructure Protection Centre

VOLUME 2 ISSUE 3

@NCIIPC

NCIIPC Newsletter

July 2018

Inside This Issue

NCIIPC taking proactive steps to raise user awareness on protection from phishing attacks.

Message from the NCIIPC Desk

Dear Readers,

Welcome to this issue of NCIIPC Quarterly Newsletter. In the previous quarter major developments were seen worldwide for release of new directives for cyber security and protection of Critical Information Infrastructure. India has published its 'Rules of Information Security Practices and Procedures for Protected System'. This aims to strengthen NCIIPC's efforts in protecting national critical assets. In a similar move in March, Australia passed bill for security of its Critical Infrastructure.

During last week of May 2018, European Union has declared General Data Protection Regulation (GDPR) to protect the Data of its citizens. The move will have its effect worldwide. Under GDPR, companies need to nominate a Data Protection Officer and implement necessary measures for data privacy. On the other side, The Internet Engineering Task Force (IETF) finalized the release of Transportation Layer Security (TLS) 1.3 version protocol. TLS 1.3 will speed up and improve the security of HTTPS protocol.

During the previous quarter, evolution of malwares targeting Indian Critical Infrastructure entities was observed. These malwares typically use various Phishing techniques to penetrate sensitive network. As a precautionary measure, NCIIPC is taking proactive steps to raise user awareness on protection from such phishing attacks.

NCIIPC organised cyber security sensitisation workshops at Chandigarh and Puducherry in collaboration with respective State Governments.

Thanks to all our readers for their participation. Kindly keep mailing your suggestions and contributions at newsletter@nciipc.gov.in

News Snippets - National

Rules Defined for Information Security of the 'Protected System'

http://www.nciipc.gov.in/documents/Rules_procedures_new2018.pdf

Central Government has declared 'Rules for the Information Security Practices and Procedures for Protected System'. The organisation having 'Protected System' shall:

- Constitute an Information Security Steering Committee (ISSC) which shall be the apex body.
- Nominate a Chief Information Security Officer (CISO).
- Maintain and continually improve Information Security Management System (ISMS) of the 'Protected System'.
- Ensure that the network architecture of 'Protected System' is documented.
- Maintain the documentation of authorised personnel having access to 'Protected System'.
- Maintain and review the documents of inventory of hardware and software related to 'Protected System'.
- Ensure that Vulnerability/Threat/Risk (V/T/R) Analysis for the cyber security architecture of 'Protected System' be carried out at least once a year.
- Implement and continually improve Cyber Crisis Management Plan (CCMP).
- Ensure conduct of internal and external Information Security audits periodically.
- Maintain and review documented process for IT Security Service Level Agreements (SLAs).
- Establish a Cyber Security Operation Centre (C-SOC).
- Establish a Network Operation Centre (NOC).
- Maintain and review the process of taking regular backup of logs of networking devices, perimeter devices, communication devices, servers, systems and services supporting 'Protected System'.

The organisation having 'Protected System' shall constitute an Information Security Steering Committee (ISSC) which shall be the apex body.

The CISO will be responsible for implementing the security measures suggested by NCIIPC.

The CISO will be responsible for implementing various security measures and share any change related to 'Protected System' with NCIIPC. He shall also establish process of sharing of relevant logs, records of Cyber Security Operation Centre (SOC) pertaining to the 'Protected System'.

Ransomware Attack on UHBVN Billing Data

Source: http://www.newindianexpress.com

On March 22, computers screens of 'Uttar Haryana Bijli Vitran Nigam' flashed a message in which hackers demanded ransom in Bitcoins in order to retrieve the data. UHBVN monitors electricity billing of nine districts of Haryana and with this cyber-attack, billing data of thousands of customers was affected. A case was registered in Panchkula under IT Act and different sections of IPC. UHVBN claimed that the cyber-attack on Automatic Meter Reading System did not affect the billing of about 4,000 Industrial consumers as backup of the same was available with the Nigam. An official of the Nigam told that there was no loss of billing data and the billing consumers would not be affected.

Hackers demanded ransom in Bitcoins in order to retrieve the data.

All Payment Operators to Store Payments Data within India Only

Source: https://rbi.org.in/

Reserve Bank of India (RBI) on 6th April directed Payments System providers to ensure that the entire data relating to payment systems operated by them is stored in India only. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. RBI has also directed Payment Operators to conduct an audit by CERT-IN empanelled auditors certifying completion of activity. "*It is observed that not all system providers store the payments data in India. In order to ensure better monitoring, it is important to have unfettered supervisory access to data stored with these system providers as also with their service providers / intermediaries/ third party vendors and other entities in the payment ecosystem*" RBI said in a notification.

"In order to ensure better monitoring, it is important to have unfettered supervisory access to data stored with these system providers." - RBI

Tamil Nadu Conducting Security Audit of Government Websites

Source: http://www.newindianexpress.com

Tamil Nadu State e-government Agency is conducting a cyber security audit of state government websites and IT applications to protect State's Critical Information Infrastructure from cyber-attack. NCIIPC had earlier advised to identify the Critical Information Infrastructure of the State which initiated the action of conducting cyber security audit.

No Confirmed Data Leakage Established - EPFO

Employees' Provident Fund Organisation, India
कर्मचारी भविष्य निधि संगठन, भारत
Ministry of Labour & Employment, Govt. of India / श्रम एवं रोजगार मंत्रालय, भारत सरकार

Source: https://www.ndtv.com

Employees' Provident Fund Organisation (EPFO) said that there was no data leakage from its data centre. The statement from EPFO came after news reports suggested that the retirement fund body had informed the Ministry of Electronics and IT of a 'data theft'. EPFO also informed that it has taken advance action by 'closing the server and host service through Common Service Centres pending vulnerability checks as part of the data security and protection'. Further it added that 'No confirmed data leakage has been established or observed so far. As such, there is nothing to be concerned about the news item. EPFO is continuously monitoring and will continue to be vigilant about it in future'.

"No confirmed data leakage has been established or observed so far. As such, there is nothing to be concerned about the news item."
- EPFO

News Snippets - International

Critical Vulnerabilities Discovered in OPC UA Industrial Protocol

OPC FOUNDATION
The Industrial Interoperability Standard™

Source: https://www.informationsecuritybuzz.com

OPC UA is an industrial protocol for reliable and secure data transmission between various systems on an industrial network. This protocol is widely used by major vendors in modern industrial facilities, in the manufacturing, oil and gas, pharmaceuticals industries and others. Kaspersky Lab experts analysed OPC Unified Architecture (OPC UA) and discovered that implementations of the protocol contained code design and writing errors. Overall, 17 zero-day vulnerabilities were identified and reported to the developers. These vulnerabilities could result in heavy damage to industry. There was risk of Denial-of-Service to industrial systems by disrupting or shutting down industrial processes. The remote code execution vulnerability allows attackers to send any kind of server commands to control industrial processes, or continue their intrusion into the network.

This protocol is widely used by major vendors in modern industrial facilities, in the manufacturing, oil and gas, pharmaceuticals industries and others.

US Company Fined for Noncompliance with Security Standards

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Source: https://www.tripwire.com/

A US-based power company has been given a notice of penalty regarding non-compliance with cybersecurity standards.

The data was exposed publicly on the Internet for 70 days which includes the usernames of the database and its cryptographic information.

The notice states that a security researcher discovered more than 30,000 asset records of the company accessible online, including information such as IP addresses and server host names. The data was exposed publicly on the Internet for 70 days which includes the usernames of the database and its cryptographic information. This would increase the risk of a malicious attacker gaining both physical and remote access to the Critical Systems. The company has agreed to pay a $2.7 million penalty, if approved, the multimillion-dollar fine would be the largest ever in the energy industry involving compliance with cybersecurity regulations.

Australia Passed the Security of Critical Infrastructure Bill

Source: https://www.zdnet.com/

Australia's Parliament passed the Security of Critical Infrastructure Bill to protect the electricity, gas, ports, and water sectors from 'foreign involvement'.

Australia's Parliament passed the Security of Critical Infrastructure Bill in March 2018 to protect the electricity, gas, ports, and water sectors from 'foreign involvement' that could lead to espionage, sabotage, and coercion. It also gives Ministers the power to direct companies to conduct risk mitigation actions. Under s32(2), the Australian Security Intelligence Organisation can provide advice to the Minister in the form of a security assessment, with the Minister then able to 'direct critical infrastructure owners or operators to do or not do a certain thing to mitigate a risk that has been identified as prejudicial to security'. The government also launched Critical Infrastructure Centre last year that works across electricity, water, ports, and telecommunications to conduct national security risk assessments and make suggestions for mitigation strategies.

Edwin Verin/Shutterstock.com

The Government Accountability Office (GAO) identified weaknesses in NASA's IT management practices for strategic planning, workforce planning, governance, and cybersecurity.

Investigators Slam NASA for Cybersecurity Shortcomings

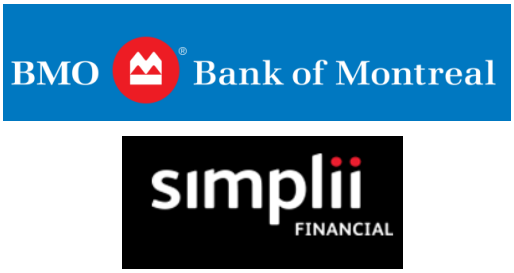
Source: https://www.nextgov.com/

Recent reports from the Government Accountability Office (GAO) identified weaknesses in NASA's (National Aeronautics and Space Administration) IT management practices for strategic planning, workforce planning, governance, and cybersecurity. GAO found that the agency's IT strategy fails to comply with Government best practices. The Chief Information Officer (CIO) planned to develop and begin implementing an agency wide cybersecurity strategy by September 2016, but investigators said that no such plan has been drafted. NASA's CIO told GAO that the agency will soon begin rolling out a strategy based on the National Institute of Standards and Technology's cybersecurity framework. The NASA Inspector General also highlighted numerous shortcomings in the Security Operations Centre, which was founded in 2007 with the intent of becoming the agency's 'cybersecurity nerve centre'.

Canadian Banks Warn: Hackers Might have Stolen Data

Source: http://www.cbc.ca/

On May 28, two major Canadian banks: Bank of Montreal and online bank Simplii Financial — owned by Canadian Imperial Bank of Commerce (CIBC) warned that hackers might have accessed the personal and financial information of nearly 90,000 customers. Hackers threatened to make this information public unless the lenders pay a $1-million ransom in cryptocurrency 'Ripple'. In an email the hackers said that they accessed information such as names, account numbers, passwords, security questions and answers, and even social insurance numbers and account balances, by exploiting weaknesses in the two banks' security systems. They used algorithm to get account numbers, which allowed them to pose as authentic account holders who had simply forgotten their password which was apparently enough to allow them to reset the backup security questions and answers, giving them access to the account. Both banks are in contact of those who have been affected and are providing instruction on how to monitor their accounts for suspicious activity.



Hackers threatened to make this information public unless the lenders pay a $1-million ransom in cryptocurrency 'Ripple'.

Trends

Use of Power Lines to Steal Data from Air-gapped Computers

Source: https://arxiv.org/pdf/1804.04014.pdf

PowerHammer is a new type of attack that uses the power lines to steal data from air-gapped computers. In this case, a malicious code running on a compromised computer can control power consumption of the system by intentionally regulating the CPU utilization. Data is modulated, encoded, and transmitted on top of the current flow fluctuations, and then it is conducted and propagated through the power lines. This phenomenon is known as a 'conducted emission'. There are two versions of this attack. First, Line level power-hammering attack, in which the attacker taps the in-home powerlines that are directly attached to the electrical outlet. Second, Phase level power-hammering attack, in which the attacker taps the power lines at the phase level, in the main electrical service panel. In both versions of the attack, the attacker measures the emission conducted and then decodes the data.

The attacker measures the emission conducted and then decodes the data.

Kaspersky Threat Landscape Report for ICS

Source: https://www.automation.com/

Kaspersky Lab released a report on, 'Threat Landscape for Industrial Automation Systems in H2 2017'. Following are the main highlights:

Nearly 40 percent of all Industrial Control Systems (ICS) in energy organizations protected by Kaspersky Lab solutions were attacked by malware at least once.

- Nearly 40 percent of all Industrial Control Systems (ICS) in energy organizations protected by Kaspersky Lab solutions were attacked by malware at least once – closely followed by 35 percent of engineering & ICS integration networks.
- For all other industries (manufacturing, transportation, utilities, food, healthcare, etc.) the proportion of ICS computers attacked ranged from 26 percent to 30 percent on average.
- The vast majority of detected attacks were accidental hits.
- The sector that demonstrated the most noticeable growth of ICS computers attacked was construction, with 31 percent attacked.
- Researchers have discovered a rise in mining attacks on ICS.
- The top five countries by percentage of ICS computers attacked includes Vietnam (70%), Algeria (66%), Morocco (60%), Indonesia (60%) and China (60%).
- In 2017, 11% of all ICS systems were attacked by botnet agents.

Five Most Dangerous New Attack Techniques

Source: https://www.sans.org/

Ed Skoudis, James Lyne and Johannes Ullrich

SANS Institute researchers at RSA Conference 2018 shared what they believe to be the five most dangerous new attack techniques in cybersecurity:

Repositories and Cloud Storage Data Leakage: With vast online code repositories for collaboration and cloud data storage hosting mission-critical applications, attackers are increasingly targeting such infrastructures, looking for passwords, crypto keys, access tokens, and terabytes of sensitive data.

Big Data Analytics, De-Anonymization, and Correlation: Now the battle is shifting from hacking machines to hacking data - gathering data from disparate sources and fusing it together to de-anonymize users, find business weaknesses and opportunities.

Exploitability in ICS/SCADA: Publicly visible ICS attacks like Triton/TriSYS show capability and intent to compromise some of the highest risk components of industrial environments. Many systems in this domain lack the mitigations of modern operating systems and applications. Attackers have demonstrated they have the inclination and resource to diversify their attacks which opens up new and concerning possibilities.

Attackers Monetize Compromised Systems Using Crypto-Miners: Most commonly stolen data like credit card numbers has dropped significantly in value. Attackers will instead install crypto coin miners. These attacks are stealthier and less likely to be discovered.

Hardware Flaws: Hardware is no less complex then software and mistakes have been made just as they are made in software. Patching hardware is a lot more difficult and often not possible without replacing entire systems or suffering significant performance penalties.

Patching hardware is a lot more difficult and often not possible without replacing entire systems or suffering significant performance penalties.

IBM Banned its Staff from Using Removable Storage Devices

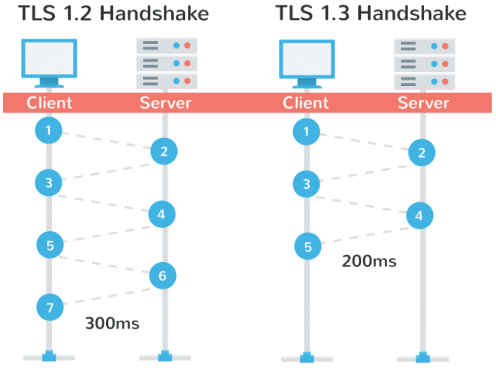
Source: http://www.theregister.co.uk/

IBM banned its staff from using removable storage devices (e.g.: USB, SD card, flash drive). The move is to minimise the possible financial and reputational damage from misplaced, lost or misused removable portable storage devices. IBM employees are advised to use company's sync 'n' share service to move data around. Parts of IBM have already been working without portable drives, but the ban now reportedly extends to all employees worldwide.

IETF Released TLS Version 1.3

Source: http://www.theregister.co.uk/

The IETF finalized Transportation Layer Security (TLS) 1.3 version after 28 drafts. TLS 1.3 protocol provides unparalleled privacy and performance compared to previous versions of TLS. With TLS 1.3, HTTPS performance has been made faster and safer for every user and every device. TLS 1.3 stopped supporting many of the older encryption algorithms that TLS 1.2 supports that over the years people have managed to find holes in. The new protocol aims to comprehensively thwart any attempts by the eavesdroppers to decrypt intercepted HTTPS connections. The new security protocol reduces latency caused during the TLS Handshake by removing a whole round-trip connection for session establishment.



The new security protocol reduces latency caused during the TLS Handshake by removing a whole round-trip connection for session establishment.

Multi-Stage Intrusion Campaign Against CII by Nation States

Sh. Mohammed Zaki Ahmed, Sectoral Coordinator, Power, NCIIPC

Recently US-CERT issued an alert on a nation state cyber activity targeting Energy, Nuclear, Commercial Facilities, Water, Aviation, and Critical Manufacturing Sectors of United States [1]. This alert refers Symantec Dragonfly reports published on 06 September 2017 [2]. Symantec has been chasing Dragonfly group since 2011, however their report of September 2017 speaks about 'Dragonfly 2.0', which is based on their assessment of group's activities since 2015. Confirmed targets of the Dragonfly campaign include US, Canada and Turkey. Dragonfly campaign is a multi-stage intrusion attack, which first targets intermediate subjects and finally compromises the Industrial Control Systems of OT.

Confirmed targets of the Dragonfly campaign include US, Canada and Turkey. Dragonfly campaign is a multi-stage intrusion attack, which first targets intermediate subjects and finally compromises the Industrial Control Systems of OT.

Motive behind the attack may be intelligence gathering, sabotage or holding backdoors for future exploitation. The attack methodology involves usage of Spear Phishing Emails, Trojan Software, and Watering Hole Websites for compromising intermediate targets. Intermediate targets may be subjects dealing with Business or IT or Safety Networks. Once the attacker has access to the Business/IT Network, it sets its Command and Control Centre (CNC-1) and tries to exploit ICS systems of the OT through various vulnerabilities such as SMB, NetBIOS; and sets up a web shell (Web/Email) server as Command and Control Centre (CNC-2), where it uploads different modules for further exploitation and communication. A secure VPN access is created for communication between victims and the CNC-2. Attackers are able to collect snapshots of the HMI Workstations of OT.

Mitigation Strategy: Organisations may thwart such attacks by following Cyber Security best practices with due diligence:

- Implement Patch Management practices for ICS components. Update firmware as and when available.
- Segregate ICS network from Enterprise or Business Network. If feasible keep the ICS systems air-gapped.
- Use multi-factor authentication such as biometric access control for allowing access to ICS/OT from other zones.
- Segregate Safety Systems such as SIS from ICS. Configure different zones through a firewall.
- Explore possibility of deploying data diodes. This will enable unidirectional data flow and may help in avoiding Command-and-Control operations of malware.
- Generate awareness in employees for Phishing Attacks and Cyber Security.

- Establish Security Operation Centre and monitor ICS traffic for security anomalies. ICS devices have a static pattern of communication over DNP/MODBUS/ICCP/IEC. Any abnormal pattern such as a device trying to connect with unknown IP Addresses should be monitored and incident alert should be issued on priority.

References:

[1] https://www.us-cert.gov/ncas/alerts/TA18-074A

[2] https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

[3] https://www.scmagazine.com/dragonfly-apt-group-may-be-prepping-to-sabotage-us-power-facilities-report-warns/article/687017/

AI in Cyber Defence: New Vista for Security Professionals

Sh. Shiv Charan Kataria, Analyst, NCIIPC

Artificial Intelligence and Machine Learning are the buzz words since last couple of years. The sophistication of technology to handle big data coupled with Machine Learning and Artificial Intelligence has simplified our lives. As businesses and Governments have already adopted Artificial Intelligence and Machine Learning, its potential to handle Cyber Security is more apparent. The sophistication and readily available technology solutions has put Hackers and businesses head-to-head. The hackers are able to develop more sophisticated threats and businesses are looking to implement Artificial Intelligence in advanced threat prevention and mitigation. Some of the usages are as follows:

As businesses and Governments have already adopted Artificial Intelligence and Machine Learning, its potential to handle Cyber Security is more apparent.

- Re-writing encryption keys continuously to enhance security.
- Auto analyse network traffic as Advanced Warning System that gives extra layer of protection.
- Identification of vulnerabilities.
- Handling of insider's threat using behavioural and policy breach analysis.

The real challenge now is to have more expertise in this field. According to Centre for Cyber Safety and Education there will be a short fall of 1.8 million cyber security professionals by 2022. Further as the existing technologies will mature, organizations will require more expertise in the field to tackle Cyber Security related issues.

This is pertinent for organizations to take advantage of this advancing AI and ML technology. To succeed in this arena, it is essential for Governments and industry to collaborate for the development of next-generation of security professionals.

References:

[1] http://www.information-age.com/shortfall-cyber-security-1-8-million-123464493/

Router-based Attacks: Next Big Trend in Cybersecurity

Sh. Niraj Vishnoi, Threat Researcher, NCIIPC

Source: https://cyf4.com

In last three months there have been series of reports pointing to attacks on Routers. On 25th May Federal Bureau of Investigation (FBI) issued an urgent bulletin [1] for anyone with a home or small office router to immediately turn it off and then turn it on again as a way to temporarily thwart the spread of foreign malware. The malware, called VPNFilter [2] targets small home and office routers. Once a router is infected, the hackers would potentially be able to use the device as a jumping-off point to launch further attacks. Talos, the security arm of Cisco reported that at least 500,000 devices in at least 54 countries have been infected. Devices manufactured by Linksys, MikroTik, Netgear and TP-Link were among those found to have been affected, according to the Talos report. Many of the infected devices have known public exploits and use default credentials, meaning that customers who set up their home router out of the box and never changed the password or updated the firmware could be at a higher risk [3].

Many of the infected devices have known public exploits and use default credentials, meaning that customers who set up their home router out of the box and never changed the password or updated the firmware could be at a higher risk.

In the month of April, United States and United Kingdom issued a joint statement that state-sponsored hackers are leveraging vulnerabilities in routers and other network infrastructure devices to target governments, private-sector organizations, infrastructure providers, and ISPs.

Kaspersky Lab reported that a targeted phishing campaign called Roaming Mantis, found primarily in South Korea, changed DNS settings on routers, pointing users to malicious websites that, in turn, prompted users to 'update' apps on Android phones to deliver a payload that harvested credentials, including those for two-factor authentication [4].

Akamai published a report detailing coordinated abuse of flawed implementations of UPnP on routers allowing hackers to inject NAT rules, creating a proxy for hackers to disguise the origin of their traffic. Akamai's report indicated 65,000 routers compromised in this way, with over 4.8 million routers potentially vulnerable [5].

In March, a report from Kaspersky Lab detailed the Slingshot malware, which targeted individuals, government agencies, and organizations located primarily in Kenya, Yemen, Libya, and Afghanistan. Mikrotik routers were leveraged in the Slingshot malware attack [6-7].

Most of these routers are at 'always-on' condition and rarely updated. Since routers play important role in normal network operations, so utilization of these devices in man-in-the-middle attacks is extremely attractive for attackers. Considering the multitude of Router models and the difficulty of supporting and updating so many devices, make these devices low hanging fruit for hackers. A compromised router can also serve as a platform for attacking other devices on your local network, such as your phone or laptop, or for launching denial-of-service attacks against Internet websites. Router exposed to the outside world, is frequently targeted by automated scans, probes and exploits. Compared to other IT devices, router doesn't have an antivirus program or other security software to protect it.

Considering the multitude of models router vendors produce and the difficulty of supporting and updating so many devices makes these devices low hanging fruit for hackers.

References:

[1] https://www.ic3.gov/media/2018/180525.aspx

[2] https://blog.talosintelligence.com/2018/05/VPNFilter.html

[3] https://www.nbcnews.com/tech/security/fbi-warns-about-russia-linked-malware-threat-home-routers-questions-n878276

[4] https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/

[5] https://www.akamai.com/us/en/multimedia/documents/white paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf

[6] https://securelist.com/apt-slingshot/84312/

[7] https://www.techrepublic.com/article/why-router-based-attacks-could-be-the-next-big-trend-in-cybersecurity/

Threat Assessment for Telecom Sector

Sh. Neeraj Saini, Sectoral Coordinator, Telecom, NCIIPC

The Telecom sector has witnessed exponential growth especially in emerging economies like India. This has resulted in rapid expansion of the network, addition of value-added services and resultant increase in complexity of the entire setup. Often, security can get overlooked or kept on the backburner in the rush to increase market share and reduce costs.

However, cyber-criminals don't care for such economic realities, and they have begun to increasingly target telecom infrastructure, especially as it becomes IP-based. This combined with increasing regulations towards telecom security have created quite a challenge that companies are seeking to address. There are varieties of security issues – some of which are solvable, while others will remain known risks till cost-feasible measures can be found to address them.

There are varieties of security issues – some of which are solvable, while others will remain known risks till cost-feasible measures can be found to address them.

Telecom Security Threats:

Major threats to Telecom Security usually fall into the following categories:

- Phone Fraud: Toll Fraud, Cramming, Telemarketing fraud, War dialling and so on
- Theft: Data theft, network abuse, illegal data interception, unauthorized data modification (in billing or routing based processes)
- Malware: Viruses, Trojan horse
- Spam: Sending spam messages via SMS, MMS
- DDoS Attacks: Distributed Denial of Service attacks constitute the great threat to the accessibility of the telecom providers. These attacks occur frequently and may target authorities, companies and citizens. DDoS attacks are carried out online and, to a lesser extent, via mobile networks, against telecom service providers, their customers, and the telecommunications infrastructure.
- Data Leakage: Penetrating billing and CRM systems to extract customer data

Typical Security Challenges:

Telecom companies face the following security challenges:

Major telecom equipment providers are not always the most security conscious infrastructure providers out there. Security hardening documentation is usually sparse and tightly held by the vendors themselves.

- Lack of Vendor's Concern: Major telecom equipment providers are not always the most security conscious infrastructure providers out there. Security hardening documentation is usually sparse and tightly held by the vendors themselves.
- Lack of Security Awareness: Many security teams in telecom companies are not aware of various security parameters in which equipments can be hardened. Equipemnts being used with default configurations causes security challenges.
- Absence of Proper Testing Setup: Few companies have proper test setups where equipment can be scanned and hardened to ensure that vulnerabilities are fixed, yet productivity isn't being hampered.

- Lack of Monitoring: Effective monitoring systems that can trace to individual operator along with details of the timestamp, system from which the command was run, and the actual user running the command must be implemented.
- Supply Chain Risks: In today's global threat landscape, government sponsored intrusions into the integrity of telecom equipment has created concerns for India. In other countries the regulators have stepped in to ensure that equipment is tested in an accredited lab.

In other countries the regulators have stepped in to ensure that equipment is tested in an accredited lab.

Threats for BFSI Sector

Sh. Aniruddha Kumar, Sectoral Coordinator, BFSI, NCIIPC

BFSI Sector remains one of the major targets of rouge actors. Based on various sources/feeds, following are some of the major attack vectors for BFSI sector:

- *Ransomware & Crypto Currencies:* In a ransomware attack, fraudsters demand ransom amount in cryptocurrencies like BitCoin etc. In last couple of years, these attacks have increased significantly, thus posing considerable risk to National Critical Information Infrastructure (NCII). Ransomware as a Service (RaaS) is also available online. So far, the most sophisticated ransomware attack in BFSI sector has been the Black Swan attack.
- *Social Engineering Attacks:* Social Engineering attacks like Phishing, Vishing, Card Skimming and Spoofing are still popular in the BFSI sector.
- *Rogue Apps:* Fraudsters are also targeting the legitimate and proprietary mobile apps developed by the financial service providers. After tweaking some of the functionalities of the Apps, the culprits are hosting these rogue Apps on third party websites other than the Google Play Store.
- *Deep Web and Dark Web:* Information like Credit/Debit cards, bank account credentials, data base leaks, internal network schema, employee details, customers detail etc. pertaining to BFSI sector is available for sale on Dark Web.

Source: http://www.channelworld.in

The information like Credit/Debit cards, bank account credentials, data base leaks, internal network schema, employee details, customers details etc. pertaining to the stakeholders of BFSI sector is available for sale on Dark Web.

Malware Bytes

Ransomware Hits HPE iLO Remote Management Interfaces

Source: https://www.bleepingcomputer.com

HPE Integrated Lights-Out (HPE iLO 4), a management processor, is under the radar of attackers. These processors are built into certain HP servers that allow administrators to remotely administer the device. One can connect to the iLO using a web browser or mobile app and will be greeted with a login page.

Shodan shows that over 5,000 iLO 4 devices are connected to the Internet and are vulnerable.

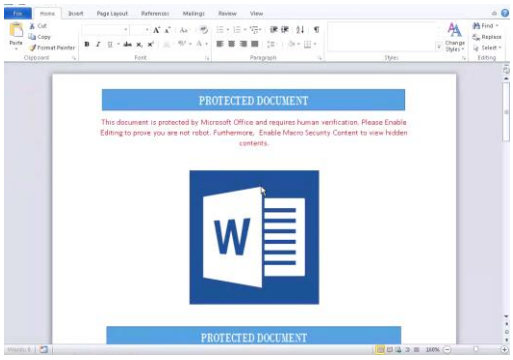
The ransomware that has been discovered recently has a 'Security Notice' at HPE iLO 4 login screen saying that the computer's hard drives are encrypted with RSA 2048 asymmetric encryption and that the owners would have to pay few Bitcoins to get the data back. Hence, it is advisable not to connect iLO 4 to the Internet (use secure VPN) as Shodan shows that over 5,000 iLO 4 devices are connected to the Internet which are vulnerable.

The cybercriminals' app installed in card chip can say a PIN is valid; no matter what PIN was entered.

Clone Chip-and-PIN Cards

Source: https://www.kaspersky.com/blog/chip-n-pin-cloning/21502/

Kaspersky researchers discovered a group of cyber crooks from Brazil who has developed a way to steal card data and successfully clone chip-and-PIN cards. Brazilian group called Prilex uses malware to infect Point-of-Sale (POS) terminals and collect card data. When a customer makes payment at a shop whose POS terminal is infected, the card data is transferred right away to the criminals. To steal money, they also needed to be able to clone cards. The Prilex group developed a whole infrastructure that lets create cloned cards. The card-cloners created an application for cards to run. The application tells the POS terminal not to perform data authentication. That means no cryptographic operations, sparing them the near-impossible task of obtaining the card's private cryptographic keys. But that still leaves PIN authentication. The app installed in card chip can say a PIN is valid; no matter what PIN was entered. That means that one can simply enter four random digits — and they'll always be accepted.



The document asks the user to enable macros in order to prove that the user is not a robot.

GravityRAT Malware Targeting Indian Entities

Source: https://blog.talosintelligence.com/

Cisco Talos reported a new piece of malware called GravityRAT. This malware has been under development for last two years, during which the developer has implemented new features like file exfiltration, remote command execution capability and anti-vm techniques. The majority of the malicious documents crafted by the malware author are Microsoft Office Word documents. The attacker uses an embedded macro in order to execute malicious code on the victim's system. The document asks the user to enable macros in order to prove that the user is not a robot. By enabling macros, the malware is able to begin its execution. The malware author uses a versioning system starting by the G letter. The oldest version we identified is G1.

All the malicious Office documents, and more specifically the documents used to test antivirus on VirusTotal, were submitted from Pakistan. It was found that across all of the C2 domains listed, a large influx of traffic was originated from India. All of the C2 domains were at least 50 percent requested by Indian IP infrastructure. This actor is probably not the most advanced actor as seen. But it managed to stay under the radar since 2016. They worked on malicious code, and produced four variants. Each new variant included new features. The developer used the same C2 infrastructure all this time. The developer was clever enough to keep this infrastructure safe, and not have it blacklisted by a security vendor. The actor took their time to ensure they were not within a virtual environment to avoid analysis. However, they did not take any time at all to attempt to obfuscate their .NET code. The code was largely trivial to reverse engineer, which meant static analysis was an easy option for this piece of malware.

All the malicious Office documents, and more specifically the documents used to test anti-virus on VirusTotal, were submitted from Pakistan.

Malware Avoids Infecting Government and Military Networks

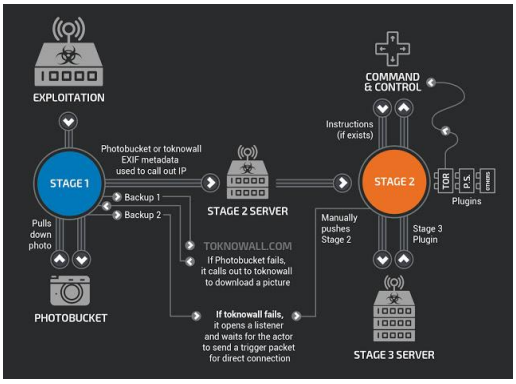
Source: https://www.bleepingcomputer.com/

Security experts have discovered a new malware GoScanSSH that targets vulnerable Linux-based systems and tries its best to avoid infecting devices on government and military networks. It scans the IP on port 22, looking for an open SSH port. If the IP has an open SSH port, the malware runs to see if the IP hosts any websites/domains of the following TLDs — .mil, .gov,. army,. airforce, .navy, .gov.uk, .mil.uk, .govt.uk, .mod.uk, .gov.au, .govt.nz, .mil.nz, .parliament.nz, .gov.il, .muni.il, .idf.il, .gov.za, .mil.za, .gob.es, .police.uk. If not, the malware uses a list of over 7,000 user-password combos to guess the SSH credentials. When the malware finds the remote device SSH credentials, it reports back to its Command & Control server located on the Dark Web (communications occur via Tor2Web proxies).

The malware uses a list of over 7,000 user-password combos to guess the SSH credentials.

VPNFilter Malware Targets at least 500K Devices Worldwide

Source: https://blog.talosintelligence.com/2018/05/VPNFilter.html



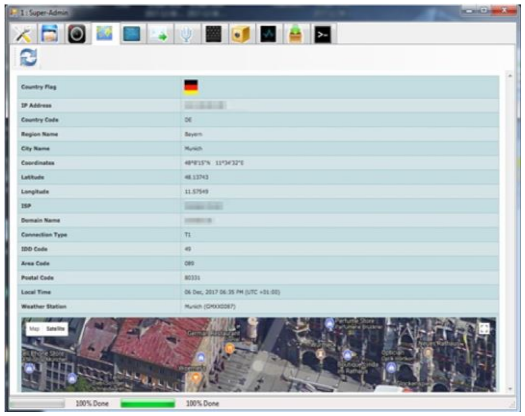
Cisco Talos reported a sophisticated modular malware called 'VPNFilter' which overlaps with versions of the Black Energy malware, which was responsible for multiple large-scale attacks in Ukraine. It is actively infecting Ukrainian hosts at an alarming rate, utilizing a command and control infrastructure dedicated to that country. Devices on the perimeter of the network, with no intrusion protection system in place, and typically no available host-based protection system such as an anti-virus package are its target. Current estimate states that at least 500,000 devices in at least 54 countries are infected. The known

The malware allows for theft of website credentials and monitoring of Modbus SCADA protocols.

devices affected by VPNFilter are Linksys, MikroTik, NETGEAR and TP-Link networking equipment in the small and home office space, as well at QNAP network-attached storage devices. The malware allows for theft of website credentials and monitoring of Modbus SCADA protocols.

APT36 (Lapis) Activity36

Source: FireEye Threat Intelligence Report APT36- 1800001788-1



APT36 (previously referred to as TEMP.Lapis and publicly referred to as Operation Transparent Tribe, ProjectM, and Operation C-Major) is a long-standing espionage team that conducts intelligence collection in support of a Nation State's military and diplomatic interests. APT36 intrusion campaigns which are active since 2013 reflect a concerted effort to target India, North Atlantic Treaty Organization (NATO) and the United Nations (UN) that have a stake in the region. Diplomatic and military personnel of India have been the target of the majority of APT36 campaigns. Open Sources indicate that Indian embassies in Saudi Arabia and Kazakhstan have also been targeted. APT36 uses social engineering emails, often spoofed to appear as if they originate from official personnel that include malicious attachments or links. APT36 has also used compromised websites as vectors for malware delivery. Spoofed personas have included an employee of an Indian news organization, Afghanistan's ambassador to the U.S., and the Afghan Minister of Finance. Malicious attachments of APT36 have leveraged Office exploits CVE-2012-0158, CVE-2015-1641, CVE-2015-1770, CVE-20103333, and CVE-2017-0199. Links direct victims to malicious payloads hosted on fake or compromised websites. APT36 employs open-source and custom malware tools that range in functionality from keystroke logging to targeting USB devices. SEEGAP malware propagates via USB, which may facilitate targeting of air-gapped networks used for sensitive military or diplomatic information. One of the APT36 malware has a feature that queries Google maps API through the registered domain 'shareboxs.net' to display information about victims' IP addresses, including satellite imagery of the region.

APT36 intrusion campaigns which are active since 2013 reflect a concerted effort to target India, North Atlantic Treaty Organization (NATO) and the United Nations (UN) that have a stake in the region.

Bus wrapped with SAP Big Data parked outside IDF13

Learning

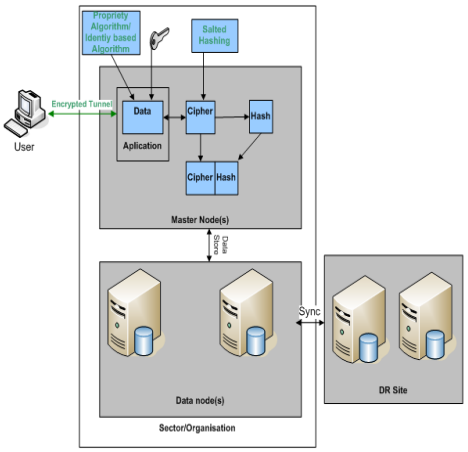
Big Data Security for Critical Information Infrastructure Protection

Sh. Navdeep Pal Singh, Sectoral Coordinator, Government, NCIIPC

Big Data has become the integral part of the CII stakeholders to carry out their day to day operational activities. However, various threat vectors get supplemented because of integration of big data with cloud storage.

Strong layered defence practices needs to be in place for protection of Big Data in CIIs.

- The architecture should be easy to deploy, manageable, scalable with security as integral part of design.
- Appropriate role based access control along with principle of least privileges should be implemented.
- Mechanism to collect and store the data in secure manner along with data validation to be done at each stage. This would help guard against masquerading and spoofing attacks.
- Data life cycle management should protect data from unauthorized access, as it passes through multiple networks, protocols, software and applications.
- Regular audit & compliance needs to be carried out.
- CII Information Security(IS) policy should cater the requirement of blocking of unused ports, hardening of the system(s)/Network appliances, prevention of exposure of critical big data network/system/component facing Internet.
- Appropriate policies and controls must be in place for rapid response, swift recovery at the time of disaster.
- Real time monitoring of all device access to detect and respond to the suspicious cyber anomalies with the help of data mining techniques and analytics.



Big Data has become the integral part of the CII stakeholders to carry out their day to day operational activities.

References:

[1] https://www.isaca.org/Groups/Professional-English/big-data/GroupDocuments/Big_Data_Top_Ten_v1.pdf

[2] http://files.technologyreview.com/whitepapers/Oracle-Securing-the-Big-Data-Life-Cycle.pdf

[3] https://cra.org/ccc/wp-content/uploads/sites/2/2015/05/bigdatawhitepaper.pdf

[4] https://www.datamation.com/big-data/big-data-security.html

Securely Using Social Media

Source: https://www.sans.org/

Social media websites allow us to interact and share information with people all around the world. However, these websites pose certain security threats as they are also used for conducting social engineering attacks. Employees or people dealing with Government, Security and other Critical Setups who are on social media are under radar of state sponsored actors.

Following are few measures which can be taken for safety:

- One must be careful about online posting. Anything posted online will get public at some point of time and may affect one's reputation. Information shared or pointers leading to sensitive information should not be divulged online.
- One must also be aware of others posting about him/her. Anything inappropriate posted by someone may be requested for removal.
- The privacy options of the different social media websites keep on changing and hence must be reviewed regularly and strong privacy options should be enabled.
- The user accounts on social media websites must be protected using strong passwords.
- Two factor authentication provides additional layer of security and should be enabled.
- One must be careful of the clicking on various links shared or downloading files. The link or contents may appear coming from a friend who might have been faked by a rogue actor.
- Users must read and review the terms of service for particular website.
- Utmost care should be maintained while posting anything related to work. Organisation should consider policy on usage of social media by its employees.

These days' social media is increasingly being used to extract confidential information, spread malware or to get entry into the trusted networks. Anything suspicious may be reported to ir@nciipc.gov.in.

These days' social media is increasingly being used to extract confidential information, spread malware or to get entry into the trusted networks. Anything suspicious may be reported to ir@nciipc.gov.in.

Port Automation and Cyber Risk

Sh. Abhijeet Raj Shrivastava, Sectoral Coordinator, Transport and Sh. Vijay Kant Verma, Analyst, NCIIPC

Ship industry is reliant on a range of electronic devices and software systems to operate efficiently in modern digital era, which includes complex cargo management systems, Automatic Identification Systems (AIS), Global Positioning Systems (GPS) and Electronic Chart Displays and Information Systems (ECDIS). Automated terminals reduce unnecessary box moves, shorten cycle times, and enables consistent and predictable throughput numbers. Fully-automated terminals have the advantage of low operating costs and reliable operations. Automation does offer major port hubs better predictability and consistency of container moves per hour.

At the same time, automation reduces the environmental impact since terminals are mostly electrified, giving ports an additional competitive edge in an industry increasingly focused on sustainability. However, full automation of port management has increased vulnerability surface to cyber risks. This is due to the use of technologically advanced and networked systems.

Full automation of port management has increased vulnerability surface to cyber risks. This is due to the use of technologically advanced and networked systems.

Cyber Risks:

- Lack or missing Cyber Crisis Management mechanism, Business continuity plan / Disaster recovery plan in ports also risk the national economy.
- The difficulty with protecting automated terminals from cyber risks lies with their complexity. These terminals use industrial control systems that translate sensorial data and commands into mechanical actions. The network links between mechanical equipment and sensors are exposed to the same threats as data networks.
- Operational systems and data networks are not always updated /patched or properly secured, allowing unauthorized actor to gain comparatively easy access to information.
- Industrial control systems are not designed with cyber risks or active network monitoring in mind. This is especially true for ships' control systems, but can also affect the system components of ports.
- Personal details of ship crews can still be easily accessed, making them more vulnerable to social engineering via phishing or other techniques, unknowingly granting access to systems.

These terminals use industrial control systems that translate sensorial data and commands into mechanical actions. The network links between mechanical equipment and sensors are exposed to the same threats as data networks.

Prevention Mechanism against Cyber Risk in Ports:

- To prevent the ports and shipping industry from most attacks, regular operating system updates, stronger passwords, secure satellite connections, resilience exercises, information sharing, and employee awareness campaigns should be practiced.
- Major shipping hubs are part of large and less resilient supply chains, which are essential for regional and international trade. These supply chains depend on a small number of key ports, which are vulnerable to shocks from other ports. To make supply chains and port hubs more resilient to cyber risks, the shipping industry as a whole will have to adjust and prepare.
- Major port operators will have to work together and share information on previous or ongoing attacks to NCIIPC and other Government organization, so that experiences and best practices can be shared directly. Agencies are able to provide incident response in time.

- Training employees actively in security protocols and procedures with information systems is one way to strengthen a port's resilience.

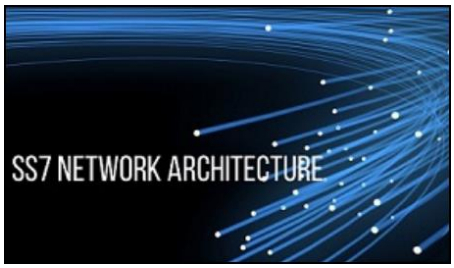
References:

[1] http://cimsec.org/port-automation-and-cyber-risk-in-the-shipping-industry/35044

[2] NCIIPC Control Guide lines.

Attack Exposure of Signalling System 7

Sh. Ashok Kumar Gupta, Analyst, Telecom, NCIIPC



Attackers could exploit security holes in SS7 to track users' movements, communications and eavesdrop on conversations.

Signalling System 7 (SS7) is an international telecommunication standard that defines how network elements in a Public Switched Telephone Network (PSTN) exchange information over a digital signalling network. Nodes in an SS7 network are called signalling points. SS7 is also called Common Channel Signalling 7 (CCS7).

Attackers could exploit security holes in SS7 to track users' movements, communications and eavesdrop on conversations as demonstrated by security researchers in Germany. The attack in question is essentially a man-in-the-middle attack on cell phone communications that, among other things, exploits the lack of authentication in the communication protocols that run on top of SS7. The possibility of Denial-of-Service attack also cannot be ruled out.

However, mobile community is working to address these threats The GSMA, security vendors and mobile operators are collaborating to better understand sophisticated adversaries' means and ways of exploiting networks. Future networks require the same degree of protection across all network types, be it GSM, CDMA or LTE. With so many people dependent on mobile devices to communicate and work, mobile network security is more important than ever.

General Data Protection Regulation

Source: https://securitycommunity.tcs.com/

The GDPR (General Data Protection Regulation) is Europe's new framework for data protection laws – it replaces the previous 1995 data protection directive. After more than four years of discussion and negotiation, GDPR was adopted by both the European Parliament and the European Council in April 2016. It came into force from 25 May 2018. While it's a European data privacy law, its impact will be felt all over the world.

Anyone involved in processing personal data about individuals in the EU (European Union) must comply, whether or not they're located in the EU, the U.S., or anywhere else in the world. The fines for companies that fail to comply can range from 2% to 4% of global yearly revenue.

The GDPR includes 99 different provisions directing companies on how to collect, manage, and process personal data while outlining key data rights for EU residents.

Major changes GDPR will bring about are:

Data Protection Officer (DPO): Companies will be required to appoint a Data Protection Officer who has independent authority to oversee a company's compliance with GDPR.

Children Protection: GDPR provide protection for children by requiring parental consent before a child's personal data can be collected by a company.

Data Breach Reporting: The GDPR mandates reporting data breaches to an EU regulator within 72 hours. That's just three days of learning of an incident. This means companies need clear escalation paths to their security and legal departments when a breach occurs.

Privacy by design: Privacy by design means thinking about data privacy and its implications when developing products, features, and marketing campaigns based on personal data.

We live in the age of data, and the GDPR marks the beginning of respecting and protecting new age gold, personal data.

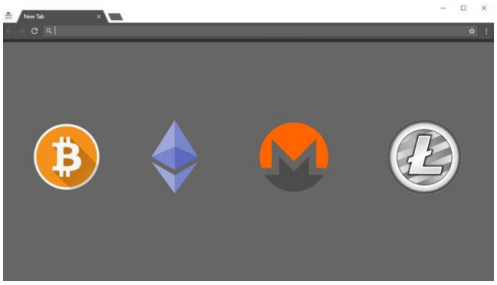
Companies will be required to appoint a Data Protection Officer who has independent authority to oversee a company's compliance with GDPR.

The GDPR includes 99 different provisions directing companies on how to collect, manage, and process personal data while outlining key data rights for EU residents.

Recent Trend Towards in-Browser Mining of Cryptocurrencies

https://arxiv.org/abs/1803.02887

Research paper published in Cornell University Library examines the recent trend towards in-browser mining of cryptocurrencies; in particular, the mining of Monero through Coinhive and similar code-bases. In this model, a user visiting a website will get a JavaScript code downloaded to his/her machine that executes at client-side in user's browser, mines a cryptocurrency, typically without user's consent or knowledge, and pays out the seigniorage to the website. Websites may consciously employ this as an alternative or to supplement advertisement revenue, may offer premium content in exchange for mining, or may be unwittingly serving the code as a result of a breach (in which case the seigniorage is collected by the attacker). The cryptocurrency Monero is preferred seemingly for its unfriendliness to large-scale ASIC mining that would drive browser-based efforts out of the market, as well as for its purported privacy features.



Source: https://fossbytes.com/

A user visiting a website will get a code downloaded to his/her machine that executes in user's browser, mines a cryptocurrency, typically without user's consent.

This landscape, conduct some measurements to establish its prevalence and profitability, outline an ethical framework for considering whether it should be classified as an attack or business opportunity, and make suggestions for the detection, mitigation and/or prevention of browser-based mining for non-consenting users.

Cyber Security Threat Assessment of Transport Sector

Sh. Abhijeet Raj Shrivastava, Sectoral Coordinator, Transport, NCIIPC

A cyber-attack on Global Positioning Systems (GPS) could significantly impact many transportation infrastructures.

Cyber threats to the Transport Sector are of concern because of the growing reliance on cyber-based control, navigation, tracking, positioning, and communications systems, as well as the ease with which malicious actors can exploit cyber systems serving transportation [1]. For example, a cyber-attack on Global Positioning Systems (GPS) could significantly impact many transportation infrastructures.

Aviation: In the aviation industry, technical advances in navigation systems and airframe design have reduced the chances of an accident; however, the increasing reliance on computers poses a different kind of threat. Traditionally air gapped Air Traffic Control network considered to be the backbone of aviation industry. But due to operational efficiency and for faster communication these are now interfacing with IT network and hence opened up a cyber-attack vector that need to be guarded strongly.

Railway: As the rail industry adapts and becomes increasingly dependent on electronic sensors and network technologies, new vulnerabilities to physical networks may unfold [2]. Cyber systems are used in rail transport and metro network for communications-based automatic train control. These systems control train movement, deliver power to the network, control signalling infrastructure, report on the condition of the rolling stock and associated infrastructure, support operational planning and timetabling.

Shipping: Cyber-attack impacting marine transportation can involve navigation, cargo control, and other industrial processes, threatening lives, the environment, property, and disrupting trade activity. Port operations such as raising a drawbridge, controlling traffic lights, scheduling trucks, and controlling pumps, values, and pipelines for delivery of fuel and liquid cargo to ships can be impacted.

Refernces:

[1] IBM X-Force security research report entitled, "Security Trends in the Transportation Industry"

[2] https://riskcenter.wharton.upenn.edu/wp-content/uploads/2018/03/WP201802_Cyber-Security-Transportation-Sector.pdf

Vulnerability Watch

MySQL for PCF is Prone to Information-disclosure Vulnerability

https://nvd.nist.gov/vuln/detail/CVE-2016-0898

MySQL for PCF is prone to information-disclosure vulnerability (CVE-2016-0898). MySQL for PCF 1.7.x versions prior to 1.7.10 are vulnerable and were discovered to log the access key in plaintext. These credentials were logged to the Service Backup component logs, and not the system log, thus were not exposed outside the Service Backup VM. It has a CVSS 3.0 Base Score of 10. Attackers can exploit this issue to obtain sensitive information that may aid in further attacks. Users of affected versions should upgrade MySQL for PCF to 1.7.10 or later.

MYSQL FOR PCF

MySQL for PCF 1.7.x versions prior to 1.7.10 were discovered to log the access key in plaintext.

Critical Vulnerability in 'Sandbox' Component of Apple macOS

https://www.cvedetails.com/cve/CVE-2018-4091/

An issue was discovered in certain Apple products. macOS before 10.13.3 is affected. The issue involves the 'Sandbox' component. It allows bypass of a sandbox protection mechanism. The App Sandbox in macOS helps ensure that apps do only what they're intended to do. App sandboxing isolates apps from the critical system components of. Even if an app is compromised by malicious software, sandboxing automatically blocks it to keep computer safe. macOS delivers sandboxing protection in Safari by sandboxing the built-in PDF viewer and plug-ins such as Adobe Flash Player, Silverlight, QuickTime, and Oracle Java.

It allows bypass of a sandbox protection mechanism.

Critical Vulnerability in Bomgar Remote Support Portal

https://nvd.nist.gov/vuln/detail/CVE-2017-12815

Path Traversal vulnerability (CVE-2017-12815) was found in a component of the Bomgar Remote Support Portal (RSP). The affected component is a JavaScript applet that is hosted at https://domain/api/content/JavaStart.jar on the vulnerable RSP deployments. The JavaStart version 52790 and prior are vulnerable. It has a CVSS 3.0 Base Score of 10.0. Successful exploitation results in file creation/modification/deletion in operating system and with privileges of the user that ran the Java applet.

BOMGAR™

Successful exploitation results in file creation/modification/ deletion in the operating system.

Code Execution Vulnerability in Atlassian Bitbucket Server

Source: https://confluence.atlassian.com/

A critical vulnerability has been found in Atlassian Bitbucket Server (CVE-2018-5225). It has a CVSS 3.0 Base Score of 9.9.

Atlassian Bitbucket

An authenticated user of Bitbucket Server could gain remote code execution.

In this; an authenticated user of Bitbucket Server could gain remote code execution using the in-browser editing feature via editing a symbolic link within a repository. Versions affected are 4.13.0, 5.5.0, 5.6.0, 5.7.0 and 5.8.0. Its impact is known to affect confidentiality, integrity, and availability. Users are advised to upgrade to latest version.

Have hard coded credentials which lead to a weak authentication vulnerability

Critical Vulnerability in Versions of QuicDoc and Office Therapy

Source: https://blog.rapid7.com/

QuicDoc & Office Therapy, a suite of software used in medical billing and documentation produced by DocuTrac, Inc., that ship with DTISQLInstaller.exe have hard coded credentials which leads to a weak authentication vulnerability (CVE-2018-5551). Versions 1.6.4.0 and prior are vulnerable. It has a CVSS 3.0 base score of 10.0. As an impact it is known to affect confidentiality, integrity, and availability.

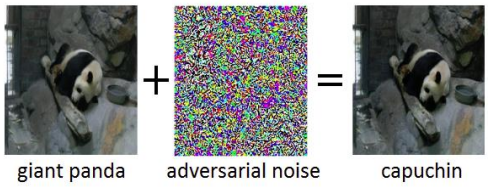
A remote attacker could exploit this vulnerability to read contents of a file

Critical Vulnerability in Versions of I-librarian

https://github.com/mkucej/i-librarian/issues/116

I-librarian version 4.8 and earlier contains XML External Entity (XXE) vulnerability (CVE-2018-1000124). It has a CVSS 3.0 Base Score of 10.0. I-librarian could allow a remote attacker to obtain sensitive information, caused by improper handling of XML external entity (XXE) by the simplexml_load_string function in importmetadata.php. By posting XML in the parameter form_import_textarea, a remote attacker could exploit this vulnerability to read contents of a file on the target host and conduct an SSRF attack.

Security App



The adversarial example on the right was obtained by adding adversarial noise (middle) to a clean input image (left). While the added noise in the adversarial example is undetectable to a human, it leads the deep neural network to misclassify the image as "capuchin" instead of "giant panda."

IBM Releases Open Source AI Security Tool

Source: https://www.securityweek.com/

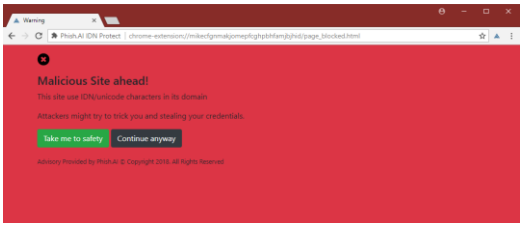
IBM Research Ireland released an open source software library, named 'Adversarial Robustness Toolbox' (ART) at the RSA Conference 2018 in San Francisco. The purpose of this library is to defend Deep Neural Networks (DNNs) against Adversarial Attacks. DNN is the machine learning model inspired by the human brain. DNN can be used for identifying objects in an image, translations or finding vulnerability in software. However, the DNN model is vulnerable to Adversarial Attack wherein system is given specially crafted input to make it mistake. The ART library written in Python uses state-of-the-art algorithms for creating adversarial examples as well as novel defence techniques for defending DNNs.

The primary intention of the library is to improve the adversarial attacks against visual recognition systems and other data modes such as speech, text or time series will be taken into account in future.

PhishProtect Beta

Source: https://www.bleepingcomputer.com/

The team from Phish.ai has released a Google Chrome extension that can detect when users are accessing domains spelled using non-standard Unicode characters and warn the users about the potential of a homograph attack. Some browsers have fought back by replacing the Unicode characters with Punycode, an ASCII-based representation of Unicode characters. For example, instead of coịnbase.com, some browsers like Edge or Vivaldi will show xn--conbse-zc8b7m.com instead, clearly highlighting that there's something wrong with the URL. But Chrome and Firefox do not show the Punycode version of the URL by default. Chrome, displays the URL Punycode version in the title bar, but not the address bar. This is where Phish.ai's extension comes to help, by showing a big red window every time the user is attempting to access a domain containing Unicode characters.

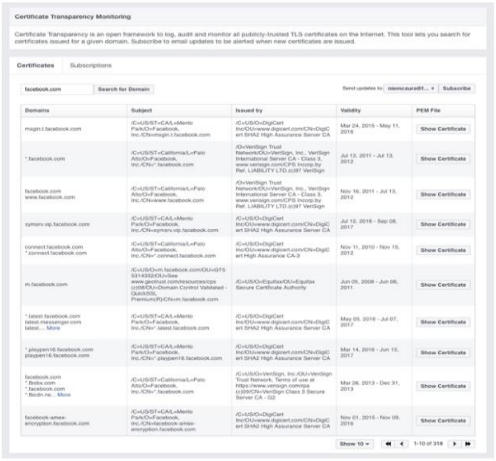


Warn the users about the potential of a homograph attack.

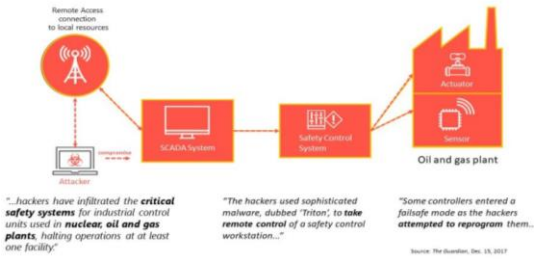
Detecting Phishing Domains using Certificate Transparency

Source: https://www.facebook.com/

Facebook released 'Certificate Transparency Monitoring Tool' which is used to detect mis-issued TLS certificates. This tool allows anybody to search observed certificates via CT logs and subscribe to domains one might be interested in monitoring. Facebook has extended the capabilities of this tool by sending alerts when certificates are issued for potential phishing domains. Whenever a new certificate appears in any public Certificate Transparency Log, the tool analyses the domains specified by the certificate for phishing attempts by taking into consideration the most common spoofing techniques — such as homograph attacks, combo squatting, typo-squatting etc. If the domain looks suspicious, i.e., likely associated with phishing, it can notify subscribers.



Certificate Transparency Monitoring tool returning certificate results for facebook.com



Microsoft demonstrated a new project codenamed Trusted Cyber Physical Systems to provide security for Internet of Things and Industrial Control Systems devices.

Trusted Cyber Physical Systems

Source: https://blogs.windows.com/

Against the backdrop of recent attacks with Trisis/Triton malware, Microsoft has demonstrated a new project codenamed Trusted Cyber Physical Systems (TCPS) at Hannover Messe 2018 in Germany to provide security for Internet of Things (IoT) and Industrial Control Systems (ICS) devices. It is a tri-component system where the first one is a hardware-level Trusted Execution Environments (TEEs) such as Intel SGX, ARM TrustZone, and SecureElements which process highly-sensitive information. The second one is a graphical user interface (GUI) which according to Microsoft is a 'Secure Confirmation Terminal' operated by a trusted employee. The third and last one is a cloud-based platform that could be used for provisioning, key management, certificate authority, patch management, and tamper-proof logging. Also, one of the most important properties of TCPS is protection for data in execution— by utilizing TEEs.

NCIIPC Initiatives

Integrity Checker

NCIIPC has developed a windows based utility named 'Integrity Checker' to calculate and verify the hash of any file input. Hash value, considered as the fingerprint of a file is processed through cryptographic algorithm. If contents of file are altered in any way, the hash value will be significantly different. This utility supports MD5, SHA1, SHA128, SHA256, SHA384 and SHA512 functions and can work across various windows platforms. It is also easy to be operated by personnel with limited exposure to technology.

NCIIPC at India-U.S. Cooperation on Global Security

National Institute of Advanced Studies (NIAS) and the Committee on International Security and Arms Control (CISAC) have been engaged in the dialogue process on a regular basis and have been discussing issues of mutual security and safety involving nuclear non-proliferation, nuclear safety, space security issues, cyber security, missile proliferation and terrorism. This year's Dialogue under the title of Strategic Threats of the 21st Century was held on 2-4 May at Bangalore. NCIIPC actively participated in the dialogue. There were more than 30 speakers and participants from various organisations like NPCIL, DRDO, ISRO, ECIL and CAPS. Various topics including disaster management, nuclear safety, cyber security, quantum computing, election security and nuclear & missile proliferation were discussed during the discussion.

NCIIPC at West Bengal's Cyber Security Awareness Workshop

A national level workshop on 'Knowledge Exchange on Awareness generation and Capacity Building in Cyber security domain' was organized at Biswa Bangla Convention Centre in Kolkata on 16th March 2018 for promoting Cyber Security Awareness in the State. Chief Guest for the event was Sh. Bratya Basu, MIC DIT&E, Government of West Bengal. NCIIPC representative delivered talk on 'Key initiatives taken by NCIIPC for CII Protection'. During the talk role, mandate and functions of NCIIPC were discussed. Focus was made on Identification of Critical Information Infrastructure in States and declaring them as protected system under Section 70 of IT act.

Sectoral Coordinator, NCIIPC delivered talk on 'Key initiatives taken by NCIIPC in terms of CII Protection'

Responsible Vulnerability Disclosure Program

The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in Critical Information Infrastructure. NCIIPC acknowledges the following researchers for their contributions towards disclosure of vulnerabilities for protection of National Critical Information Infrastructure:

- Sh. Amrendra Sharan
- Sh. Roshan Pathak
- Sh. Srinivas Kodali
- Sh. Abhilash Mohanrao Gangane
- Sh. Apurv Singh Gautam
- Gsociety01
- Sh. Rachna Khaira
- Sh. Akshay
- Sh. Mayank Bhatia
- Sh. Abhay Rana
- Sh. Sudhakar Verma
- Sh. Vijay Kumar

NCIIPC acknowledges the researchers for their contributions towards protection of National Critical Information Infrastructure.

Punjab Organizes Workshop on Information Security with NCIIPC

Department of Governance Reforms, Punjab in collaboration with NCIIPC organised 2nd 'Information Security Sensitization Workshop on Critical Information Infrastructure Protection' on 18th May at Chandigarh. Shri Parminder Pal Singh, Director/CISO, Department of Governance Reforms, Government of Punjab delivered the welcome address.

DDG, NCIIPC delivered inaugural address

The event was inaugurated by Deputy Director General (DDG), NCIIPC. Roles and Responsibilities of NCIIPC to protect the National Critical Information Infrastructure, Cyber Hygiene and Best Practices, Mapping of Attack Vectors to NCIIPC Control Guidelines v2.0 and NCIIPC Initiatives and Services were some of the key talks delivered by NCIIPC officials. Officers from Critical Sectors of Punjab viz. PSPCL (Punjab State Power Cooperation Limited), Transport, Punjab Police, State Data Centre and PAWAN (Punjab State Wide Area Network) also delivered talks on their cyber security framework and had fruitful discussions regarding risk assessment, gap analysis and additional mitigation controls. NCIIPC and Punjab Government to further collaborate to identify and notify CIIs of the Punjab State including formation of Information Security Steering Committee (ISSC).

Director NCIIPC at a workshop in Puducherry

NCIIPC and Puducherry Jointly Organised One Day Workshop

NCIIPC and Department of Information Technology, Puducherry jointly organised workshop on Critical Information Infrastructure Protection. The event was held on 23rd March 2018. The workshop was inaugurated by M.O.H.F Shahjahan, IT Minister, Government of Puducherry.

DG, NCIIPC at FICCI Homeland Security 2018

NCIIPC at FICCI Homeland Security 2018

FICCI on an annual basis organises conference on Homeland Security aimed to bring together stakeholders from the Government, Intelligence & Police Forces, Industry, Academia & Think Tanks to promote development and implementation of systems and concepts to combat cyber-crime, encourage 'Make-in-India' for Cybersecurity and provide platform to Indian start-ups for understanding the requirements of Government agencies and support them to promote indigenous expertise in cyber security. The theme of this year's programme organised by FICCI along with VIF India during 30-31 May was 'Cyber Crime Management'. The event was inaugurated by Sh. S.S. Ahluwalia, Union Minister of State for Electronics and IT, Government of India. Amongst the key speakers was Sh. Alok Joshi, Chairman NTRO who spoke on 'Next Generation Cyber Technologies for Homeland Security'. Dr Ajeet Bajpai, DG NCIIPC chaired the session on 'Technology for Protecting CII'.

Upcoming Events - Global

July 2018

- International Conference on Cybercrime and Computer Forensics, Malaysia 1-4 Jul
- OWASP AppSec Europe 2018, London 2-6 Jul
- Cyber Security for Financial Services, Colombo 10-11 Jul
- 13th International Conference on Internet Monitoring and Protection, Barcelona 22-26 Jul
- IEEE International Workshop on Secure Digital Identity Management, Tokyo 23-27 Jul
- RSA Conference Asia Pacific & Japan, Singapore 25-27 Jul
- Global Cyber Security Summit, Kathmandu 27-28 Jul
- IEEE International Conference on Blockchain, Halifax 30 Jul-3 Aug

August 2018

- Black Hat, USA 2018 4-9 Aug
- 14th EAI International Conference on Security and Privacy in Communication Networks, Singapore 8-10 Aug
- DEF CON 26, Las Vegas 9-12 Aug
- CISO Healthcare Connect, Florida 15-17 Aug
- Global CISO Executive Summit, South Carolina 20-22 Aug
- Cybercon Asia 2018, Philippines 25-26 Aug
- 12th International Conference on Network and System Security, Hong Kong 27-29 Aug
- International Symposium for ICS & SCADA Cyber Security Research, Hamburg 29-30 Aug

September 2018

- International Workshop on Cyber Security for Intelligent Transportation Systems, Barcelona 6-7 Sep
- Annual Cyber Senate Industrial Control Cyber Security Conference, Sacramento 18-19 Sep
- Kaspersky Industrial Cybersecurity, Sochi 19-21 Sep
- International Conference on Critical Information Infrastructures Security, Kaunas 24-26 Sep
- 14th International Conference on Information Security Practice and Experience, Tokyo 25-27 Sep

JULY 2018

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

AUGUST 2018

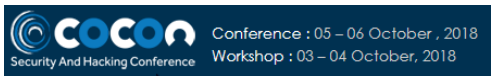
S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

SEPTEMBER 2018

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

OCTOBER 2018

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			



October 2018

- Cyber Security for Critical Assets, London 2-3 Oct
- AppSec USA, San Jose 8-12 Oct
- Annual Industrial Control Cyber Security, London 9-10 Oct
- ATM & Cyber Security, London 9-10 Oct
- International Conference on Security of Smart Cities, Industrial Control System and Communications, Shanghai 18-19 Oct
- ICS Cyber Security Conference, Atlanta 22-25 Oct
- International Summit on Cyber Security in SCADA and Industrial Control Systems, Stockholm 22-25 Oct
- Cybersecurity for Industrial Environments and Critical Infrastructures, Manchester 23-25 Oct
- ACS/IEEE International Conference on Computer Systems and Applications, Aqaba 28 Oct - 1 Nov
- US China Blockchain and Digital Currency Conference, Las Vegas 30 Oct

Upcoming Events - India

- SANS Cyber Defence Bangalore 2018 23–28 Jul
- Shared task on Detecting Malicious Domain Names, Bangalore 19-22 Sep
- c0c0n, Kochi 5-6 Oct
- HAKON - International Information Security Meet Indore 7 Oct
- First International Conference on Secure Cyber Computing and Communication, Jalandhar 11-13 Oct
- International Conference on Cyber Security, Jaipur 26-17 Oct
- 21st Association of Anti-Virus Asia Researchers Conference 2018, Goa 28-30 Nov
- Cyber Security India, Hyderabad 4-5 Dec
- SPACE 2018 — Conference on Security, Privacy and Applied Cryptography Engineering, Kanpur 17-19 Dec

General Help helpdesk1@nciipc.gov.in
helpdesk2@nciipc.gov.in

Incident Reporting : ir@nciipc.gov.in

Vulnerability Disclosure : rvdp@nciipc.gov.in

Malware Upload : mal.repository@nciipc.gov.in

Feedback/Contribution

Suggestions, feedback and contributions are welcome at newsletter@nciipc.gov.in

Disclaimer

NCIIPC does not endorse any vendor, product or service. The content of the newsletter is for informational purpose only. Readers may validate the information on their own.