NEWSLETTER

January 2020

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

VOLUME 4 ISSUE 1

@NCIIPC

NCIIPC Newsletter

January 2020

Inside This Issue

NCIIPC has now established its Zonal Office (West) at Mumbai for better coordination with Critical Sector Entities in West Zone.

Message from the NCIIPC Desk

Dear Readers,

NCIIPC wishes its readers a very prosperous and secure 2020. The Newsletter has successfully completed three years. It is heartening to witness an exponential rise in readership, both within the country and globally, as discerned from downloads of the NCIIPC website. It has been our constant endeavor to keep our readers updated about the trends, threats and challenges in Critical Information Infrastructure Protection.

Sophistication of recent attacks on critical sector entities across the world is an eye-opener and a wake-up call for us to take serious note of the emerging cyber security threats. Malwares have evolved from simple viruses, worms, trojans, spywares etc. to high end Ransomwares, Bots and Cryptocurrency Miners.

Cyber criminals are now increasingly switching to Homograph Attacks using Punycode. NCIIPC has successfully integrated various techniques for early stage detection of Homograph Attack and developed Plug-ins for Chrome and Firefox Browsers. 'PunyCodeChecker' Plug-In developed by NCIIPC for Chrome and Firefox browsers is available on 'Chrome Web Store' and 'Firefox Browser Add-Ons' respectively.

Windows 7 and Windows Server 2008 Operating Systems (OS) are on end-of-support from 14 January 2020 and no security updates shall be released by Microsoft for them. Organisations, especially the ones having Critical Information Infrastructure (CII) would run a very high risk in case they fail to replace/upgrade their systems at the earliest to prevent attacks.

NCIIPC has now established its Zonal Office (West) at Mumbai for better coordination with Critical Sector Entities in West Zone.

Comments, suggestions and feedback are solicited from the readers. Selected letters shall also be published. You may write to us at newsletter@nciipc.gov.in

News Snippets - National

Punjab sets up Digital Investigation Unit to counter Cyber Terror

Source: https://www.dailypioneer.com

A state-of-the-art Digital Investigation Training and Analysis Centre (DITAC) was inaugurated by Punjab Government on 9th September 2019 to strengthen its anti-terror capabilities in face of growing cyber terror threat. It is the fourth such establishment in the country, with other three units established in Gurugram, Guwahati and Dehradun respectively. The facility is set up at the State Cyber Crime Cell as a collaborative venture between the Punjab Police and National Technical Research Organization (NTRO). It would help scale up the state's operational preparedness in the field of cyber forensics, social media analytics and cryptology. It would also help the law enforcement agencies to further develop expertise in effectively countering anti-social elements in cyber space, besides extending quality training to police personnel in the field of strategic cybercrime monitoring. The center is equipped with sophisticated tools and software that would aid in investigation and detection of crime online.

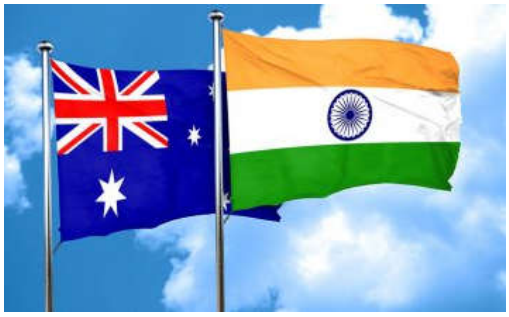
Image Source: https://punjabikhurki.com

It is the fourth such establishment in the country, with other three units established in Gurugram, Guwahati and Dehradun.

India-Australia affirm commitment to Security in Cyber Space

Source: https://mea.gov.in

The third India-Australia Cyber Policy Dialogue was held in New Delhi on 4th September 2019. The Indian delegation was led by Shri Upender Singh Rawat, Joint Secretary in charge of e-Governance, Information Technology and Cyber Diplomacy at the Indian Ministry of External Affairs, and had consisted of representatives from NSCS, MHA, MeitY, DoT, CERT-In and NCIIPC. The Australian delegation was led by Ambassador for Cyber Affairs Dr. Tobias Feakin. The Dialogue provided an opportunity to discuss current and emerging cyber security issues including emerging ICT technologies, national approaches to cyber security policy and legislation, international issues including respective views on the UN Group of Governmental Experts and Open Ended Working Group, critical technologies, and cooperation to address cybercrime. Both countries agreed to work towards the establishment of a Joint Working Group on Cyber Security Cooperation and commencing negotiations for a Framework Agreement on Cyber Cooperation. India and Australia have committed to share information on IoT security standards and best practices.

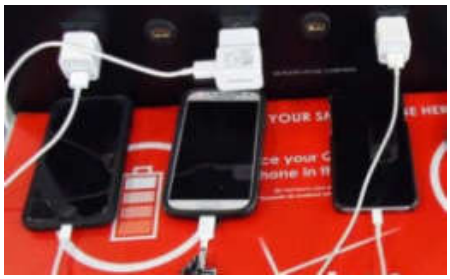


India and Australia have committed to share information on IoT security standards and best practices.

Public Phone Chargers new Hacking Hubs around Delhi-NCR

Source: https://www.indiatoday.in

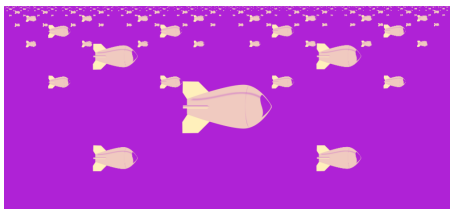
Several cases have been reported in Delhi-NCR where mobile phone's data was compromised, and criminal activities carried out, such as, amounts being debited from the bank account,



Inside the cord is an extra chip that deploys hidden malware on phone to download information without knowledge.

objectionable content posted on the social media pages without owner's knowledge, student stalked and blackmailed by the phone hacker, and so on. In all these cases one thing was found to be common, viz, they all used public USB charging cables to charge their phones. This is a rising criminal phenomenon known as Juice Jacking. Since the USB cables used for charging aren't monitored, they can be easily tampered with. The charging cables have an extra chip that deploys hidden malware on phone, which downloads information without the owner's knowledge. One must be aware that these charging cables are also designed to transfer data, not just power. Scammers are doing this mainly at airports and shopping hotspots or tourist destinations to steal bank details and other sensitive information. Phone users are advised to carry a regular charger along and plug it into a wall outlet or carry a portable power bank. One must also avoid cables that are seemingly left in USB ports by other people.

News Snippets - International



The attackers successfully managed to bring down Cool Ideas' external connections to other ISPs.

'Carpet-bombing' DDoS attack takes down South African ISP

Source: https://www.zdnet.com

Mysterious attackers took down a South African internet service provider Cool Ideas using a DDoS technique called Carpet-bombing. During this attack, all customers on Cool Ideas' network received junk traffic. The junk traffic wasn't of a large scale to bring down each customer's connection, but was large enough to overwhelm the servers of Cool Ideas' network border. Hackers sent junk traffic to unpatched DNS and CLDAP servers, which, in turn, reflected traffic towards Cool Ideas' network. The attackers successfully managed to bring down Cool ideas' external connections to other ISPs. As a result, the customers of Cool Ideas experienced intermittent connectivity loss and degraded performance for connections trying to access an international service or website.

Symantec has identified a total of 11 organizations hit by the group, majority of which are based in Saudi Arabia.

Tortoiseshell Group Targets IT Providers in Saudi Arabia

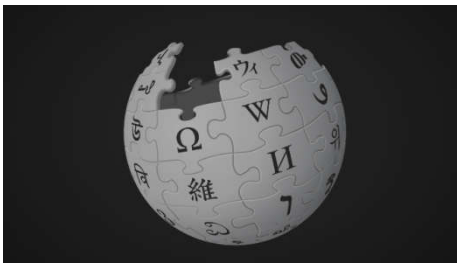
Source: https://www.symantec.com

A previously undocumented attack group dubbed as Tortoiseshell Group is using custom and off-the-shelf malware to target Saudi Arabia's IT providers. The attack appears to be a supply chain attack. Symantec has identified a total of 11 organizations hit by the group, majority of which are based in Saudi Arabia. The researchers have gathered evidence that suggests that the attackers were able to gain domain admin-level access to the networks of at least two organizations. The Tortoiseshell used a unique malware called "Backdoor.Syskit". It has been developed in both Delphi and .NET. The malware deploys several information gathering tools and retrieves a range of information about the machine and sends it to the C&C server.

Wikipedia blames Malicious DDoS Attack after Site goes down

Source: https://techcrunch.com

Wikipedia, the global encyclopaedia was hit with a cyber-attack and was offline in several countries. The attack was continuous and Wikipedia's Site Reliability Engineering team worked hard to stop the attack and restore access to the site. Users across Europe and parts of the Middle East experienced outages. "Along with the rest of the web, Wikipedia operates in an increasingly sophisticated and complex environment where threats are continuously evolving. Concerning this, the Wikimedia Foundation and Wikimedia Communities have created dedicated systems and staff to regularly monitor and address risks. When a problem occurs, it learns, improves and prepare better for the next time. These sorts of attacks are to be condemned. It's not about just taking Wikipedia offline. Takedown attacks threaten everyone's fundamental rights to freely share and access information"- Wikimedia said in the statement.



Users across Europe and parts of the Middle East experienced outages.

Georgia Hit by Massive Cyber Attack

Source: https://www.bbc.com/news/technology-50207192

A massive cyber-attack knocked out more than 2,000 websites as well as the national TV station in Georgia. Court websites containing case materials and personal data were also attacked. In many cases, website home pages were replaced with an image of former president Mikheil Saakashvili along with caption "I'll be back". More than 15,000 pages were affected, including the presidential website, private companies and non-government organisations. Imedi TV station was paralysed for under an hour while Maestro's computers and other equipment were reportedly damaged.

Website home pages were replaced with an image of former president Mikheil Saakashvili along with caption "I'll be back"

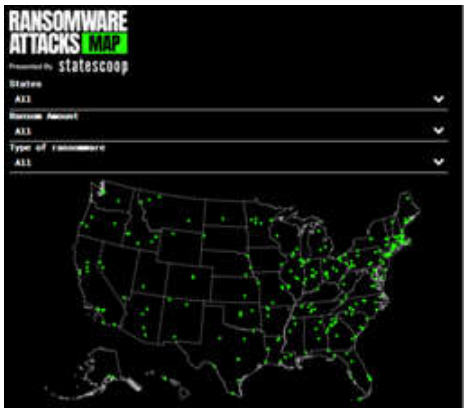
AWS left reeling after eight-hour DDoS

Source: https://www.infosecurity-magazine.com

Amazon Web Services (AWS) customers experienced severe outages after an apparent DDoS attack that took S3 and other services offline for around eight hours. The attack affected the cloud giant's router 53 DNS web service, which had an effect on other services including Relational Database Service (RDS), Elastic Compute Cloud (EC2) and Elastic Load Balancing (ELB), that requires the public DNS resolution. AWS DDoS mitigation platform Shield Advanced absorbed the vast majority of traffic, but it also flagged some legitimate customer queries making things worse for some customers. Global SVP for Neustar, Anthony Chadd said, "Citing potential mitigation concerns, this attack should serve a reminder to security leaders to ensure they safeguard their cyber-defences on an always-on basis across a number of levels, from the perimeter to websites and applications, underpinned by intelligence".

The attack affected the cloud giant's router 53 DNS web service, which had an effect on other services.

Ransomware Attacks Map chronicles a growing Threat



StateScoop has developed an interactive map of every known public-sector ransomware attack going back nearly six years.

Source: https://statescoop.com

An intelligence analyst at the cybersecurity firm Recorded Future, published research that included a list of 169 different ransomware attacks against local and state governments dating back to 2013, but now they were cropping up at an alarming rate. This research lent new insight to how broad, aggressive and increasingly common this type of malware had become. Now every few weeks there are new high-profile incidents: Baltimore; Riviera Beach and Lake City, Florida; while smaller events, many of which go unreported, strike almost daily. In order to keep track of such incidents, StateScoop has developed an interactive map of every known public-sector ransomware attack going back nearly six years. Beginning with original set of 169 attacks, StateScoop's reporters and designers have continued to track new attacks, plotting out targets and cataloguing the type of malware used, the ransom demanded and whether or not the victim paid up. Upon release, the map contains data for 245 ransomware attacks, but new dots will be added as new attacks are reported.

European Airport Systems Infected with Monero Mining Malware

Apart from affecting the infected systems' overall performance and leading to increased power consumption, the XMRig Monero miner did not impact the airport's operations.

Source: https://www.bleepingcomputer.com

More than 50% of all computing systems at a European international airport were found to be infected with a Monero cryptominer linked to the Anti-CoinMiner campaign Zscaler. The cryptojacking attack was discovered while deploying Cyberbit's Endpoint Detection and Response security solution. Apart from affecting the infected systems' overall performance and leading to increased power consumption, the XMRig Monero miner did not impact the airport's operations. While the cryptominer used to infect the airport's computers was identified over a year ago by Zscaler, the attackers modified it sufficiently enough to make sure that it would not be identified by anti-malware software. Cyberbit discovered the infection because the threat actors repeatedly launched PAExec, a redistributable version of the legitimate Microsoft tool PsExec. The tool was used for privilege escalation and it allowed them to launch an executable named Player in system mode which would provide maximum privileges. The attackers used Reflective Dynamic-Link Library (DLL) loading, a known detection evasion technique used by malware operators, to inject malicious DLLs into a host process running in memory without using the Windows loader and completely bypassing the infected systems' hard drives. PAExec was also added by the malware into the systems' registries to gain persistence to make sure that the airport employees can't get rid of the infection by rebooting the impacted computers.

Microsoft Ending Support for Windows 7 and Server 2008 R2

Source: https://www.us-cert.gov/ncas/alerts/aa19-290a

Support for Windows 7 and Windows Server 2008 R2 operating systems would end on January 14, 2020. After this date, both these products will not receive any free technical support, or software and security updates. Systems running Windows 7 and Windows Server 2008 R2 will continue to work at their current capacity even after support ends on January 14, 2020. However, using unsupported software may increase the possibility of malware and other security threats. Mission and business functions supported by systems running Windows 7 and Windows Server 2008 R2 could experience negative consequences resulting from unpatched vulnerabilities and software bugs. These negative consequences could include the loss of confidentiality, integrity, and availability of data, system resources, and business assets.

Image Source: https://www.mpsplc.co.uk/wp-content/uploads/2019/06/Windows-7-and-Server-2008-2-500x250.png

Popular Applications Hacked at Elite Chinese Hacking Contest

Source: https://www.zdnet.com

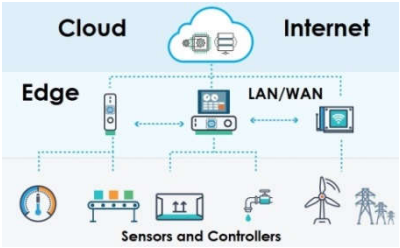
China's top hackers gathered in the city of Chengdu to compete in China's top hacking competition the Tianfu Cup- a two-day event. Chinese security researchers tested zero-days against some of the world's most popular applications. The goal was to exploit and take over an app using never-before-seen vulnerabilities. The Tianfu Cup's rules are identical to Pwn2Own, the world's largest hacking contest. Tianfu Cup organizers reported successful hacks of Microsoft Edge (the old version based on the EdgeHTML engine, not the new Chromium version), Chrome, Safari, Office 365, Adobe PDF Reader, D-Link DIR-878 router, qemu-kvm + Ubuntu, VMWare Workstation.

Trends

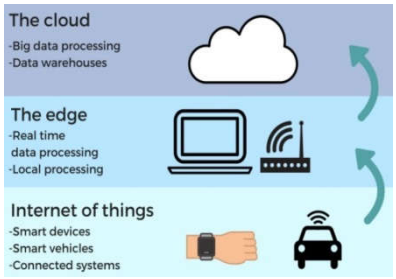
Latest Technological Trends in Data Centre

Government Sector, NCIIPC

Modern data centres are wonders of computing technology, featuring state-of-the-art high-density servers and revolutionary cooling systems. They also offer a wide range of services that are accessible to even some of the smallest start-ups, providing them with infrastructure resources that would have been unthinkable in previous decades.



Cloud computing has traditionally served as a reliable and cost-effective means for connecting many devices to the Internet, as Internet of Things (IoT) devices become more common each year, the number of devices capable of handling that processing load is increasing and continuous rise of IoT and mobile computing has put a strain on networking bandwidth. Traditional Cloud Computing requires collected



Edge computing is a distributed computing paradigm which brings computation and data storage closer to the location where it is needed, to improve response times and save bandwidth

data to travel back to the core of the network where it can be processed by the central server. Since data is constrained by the laws of physics, it doesn't travel there instantaneously, resulting in latency that slows streaming content services, medical devices, industrial scanners, and other devices.

Here Edge Computing Technology comes into picture which is now emerging to offer an alternative solution. It could be the next major trend for the data centre industry. Edge-computing architecture extends the reach of a typical cloud network by pushing key processing functions to the edge of the network, closer to where the data itself is gathered. Doing so reduces the need to transfer data back and forth between centralized computing locations such as the cloud at which edge computing is more viable than ever. It can greatly increase speed and responsiveness. Edge data centres are also being used to extend network reach and increase speed, providing more powerful processing resources that can handle tasks too big for IoT devices.

References:

[1] https://www.vxchnge.com

[2] https://www.cbinsights.com

Mobile Secure Payment- PCI SSC introduces SPoC

Source: https://www.intertek.com/blog/2019-09-03-spoc/

The SPoC standard outlines the use case where a customer can perform PIN entry directly onto a merchant's Commercial-Off-The-Shelf (COTS) touch screen smart phone or tablet.

Payment Card Industry Security Standards Council (PCI SSC) has released a new standard that tackles the ever changing landscape of mobile payment. It introduced Software PIN on COTS (SPoC). The SPoC standard outlines the use case where a customer can perform PIN entry directly onto a merchant's Commercial-Off-The-Shelf (COTS) touch screen smart phone or tablet. This could provide merchants with a more cost-effective way to accept EMV Chip & PIN payments while offering SPoC solution providers another path to expand on their secure payment offerings.

SPoC brings together PCI SSC's key standards such as the Data Security Standard (DSS), PTS and PCI PIN to ensure that all card holder data is protected throughout the whole transaction life cycle. A SPoC solution must include the following parts:

- A PTS approved Secure Card Reader for PIN (SCRP) device.
- A PIN Cardholder Verification Method (CVM) Application.
- A PCI DSS compliant and PCI PIN compliant back-end processing environment hosting the SPoC back-end.
- A back-end monitoring system that provides device status and attestations capabilities and real-time response.

Cyber-attack on Energy Sector

Sectoral Coordinator, Power and Energy Sector, NCIIPC

Critical infrastructure in Energy sectors is attractive to different threat actors. Threat actors can gain access to IT-OT systems to gather sensitive information about oil and gas companies such as facility's layout, critical thresholds, or device settings for use in later attacks. Sabotage, including disruption of services or triggering dangerous and even lethal situations involving flammable or critical resources, represent an undesirable extreme.

Nation-state attackers have typically carried out destructive cyber-attacks against the oil and gas companies. Recently, Energy Sector in Middle East has been under attack by the ZeroCleare malware. ZeroCleare is similar to the notorious Shamoon malware and it's designed to overwrite the Master Boot Record (MBR) and disk partitions of devices running Windows. Also similar to Shamoon, this new piece of malware had spread to many devices on the network of the targeted organizations, enabling the attackers to cause serious damage and it also has the potential to wipe thousands of computers.

Destructive cyberattacks against energy CII in Middle East indicate a high impact threat to both national and international markets as it has a huge petrochemical market in the world with 64.5 percent of the world's oil reserves, according to Organization of the Petroleum Exporting Countries (OPEC).

Following mitigation strategies against such sophisticated cyber-attacks may be adopted:

- Use Threat Intelligence to Understand the Risk
- Deploy Identity & Access Management
- Limit Privileged Users
- Implement Multi Factor Authentication
- Backups, Test Backups and Keep Offline Backups
- Incorporate multiple layers of security controls
- Application whitelisting
- Regular monitoring and detection in case of malware infection
- Better threat visibility and early detection of anomalies

X-Force IRIS Cyberattack Preparation and Execution Framework (Source: IBM X-Force)

Recently, Energy Sector in Middle East has been under attack by the ZeroCleare malware. ZeroCleare is similar to the notorious Shamoon malware and it's designed to overwrite the Master Boot Record (MBR) and disk partitions of devices running Windows.

References:

[1] https://www.ibm.com/downloads/cas/OAJ4VZNJ

[2] https://www.securityweek.com/iran-linked-zerocleare-wiper-targets-energy-industrial-sectors-middle-east

[3] https://www.opec.org/opec_web/en/data_graphs/330.htm

Mission of the OCA is to create a unified security ecosystem, where businesses no longer have to build one-off manual integrations between every product.

18 Cybersecurity Firms Team Up to Plug their Products Together

Source: https://www.cbronline.com/news/open-cybersecurity-alliance

Eighteen leading cybersecurity companies have teamed up to improve cross-product interoperability. The Open Cybersecurity Alliance (OCA) launched by open standards group OASIS, has brought in Cybereason, CrowdStrike, McAfee, IBM and 14 others. IBM's Jason Keirstead said that the mission of the OCA is to create a unified security ecosystem, where businesses no longer have to build one-off manual integrations between every product, but instead can build one integration to work across all, based on a commonly accepted set of standards and code. IBM and McAfee are leading the alliance and have already opened up two projects that will form part of the OCA's initial technological offering. IBM has released its STIX-Shifter onto Github: this is an open source library that can identify and format data about potential threats contained within data repositories. McAfee has developed OpenDXL- a cybersecurity messaging format.

Image Source: https://www.forbes.com

U.S. Steps Up Scrutiny of Airplane Cybersecurity

Source: https://airlinergs.com

The U.S. officials have been prompted to re-energize efforts to identify airliners' vulnerability to hacking amidst concerns that planes could be targeted in cyberattacks. The program aims to identify cybersecurity risks in aviation and improve U.S. cyber resilience in the critical area of public infrastructure. However, a stopgap, after the fact effort to evaluate security will provide only temporary benefits. To effect real and lasting change in critical infrastructure cybersecurity, the organisations that create the software products that are used in critical infrastructure must themselves be infused with secure software development practices. And of course in such a climate, increased testing can only be a good thing.

Linux to get Kernel 'lockdown' feature

Source: https://www.zdnet.com

A new security feature for the Linux kernel, named "lockdown" has been approved for inclusion. The new feature will ship as a LSM (Linux Security Module) in the Linux kernel 5.4 branch, where it will be turned off by default; usage being optional due to the risk of breaking existing systems. The new feature's primary function will be to strengthen the divide between userland processes and kernel code by preventing even the root account from interacting with kernel code. When enabled, the new "lockdown" feature will restrict some kernel functionality, even for the root user, making it harder for compromised root accounts to compromise the rest of the OS.

The lockdown module is intended to allow for kernels to be locked down early in the boot process. It will support two lockdown modes integrity and confidentiality. Each is unique, and restricts access to different kernel functionality.

The NIST Privacy Framework

Source: https://www.bankinfosecurity.com

The US National Institute of Standards and Technology (NIST) is ready to publish the first version of its Privacy Framework, a tool to help organizations identify, assess, manage and communicate about privacy risk. The privacy framework is modelled after the widely adopted, 5-year-old NIST Cybersecurity Framework, a voluntary set of guidance aimed to help mitigate cyber risk. At the core of the privacy framework is a set of privacy protection activities and outcomes. The framework consists of five functions aimed to help organization in and out of the U.S. federal government to identify, govern, control, protect and communicate about privacy.

NIST

PRIVACY FRAMEWORK

It will help organizations to identify, assess, manage and communicate about privacy risk.

The US GAO calls for stronger Strategy to Protect Grid

Source: https://www.meritalk.com

The Government Accountability Office (GAO) identified several Cybersecurity risks to the U.S. electric grid and called upon the Department of Energy (DoE) to develop an improved Federal strategy to protect against cyber threats to the grid. GAO found that threat actors – including nation states, state-sponsored groups, terrorists, and criminal groups – are increasingly becoming more capable of conducting cyberattacks on the grid. The increased attack surface is largely because of remote-access industrial control system devices, consumer Internet of Things devices connected to the grid's distribution networks, and GPS systems. DoE, the Department of Homeland Security (DHS), the Federal Energy Regulatory Commission (FERC), and other agencies have engaged in activities to protect critical infrastructure. GAO issued recommendations to DoE and FERC. Both DoE and FERC have agreed with the recommendations.

The increased attack surface is largely because of remote-access industrial control system devices, consumer Internet of Things devices connected to the grid's distribution networks, and GPS systems.

NIST defines Zero Trust Architecture, releases Use Cases

Source: https://csrc.nist.gov/publications/detail/sp/800-207/draft

Zero Trust refers to an evolving set of network security paradigms that move network defenses from wide network perimeters to narrowly focusing on individual or small groups of resources.

Zero Trust refers to an evolving set of network security paradigms that move network defenses from wide network perimeters to narrowly focusing on individual or small groups of resources.

A Zero Trust Architecture (ZTA) strategy is one where there is no implicit trust granted to systems based on their physical or network location (i.e., local area networks vs. the Internet). Access to data resources is granted when the resource is required, and authentication (both user and device) is performed before the connection is established. ZTA is a response to enterprise network trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary. ZTA focuses on protecting resources, not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.

The Malicious Macros Problem may be solved soon

Source: https://www.databreachtoday.com

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

Macros have long been enabled by default. But around two years ago, FireEye's Mandiant investigations unit wrote about attackers actually calling victims to get them to enable macros. The source of the problems is usually the macros, the powerful code snippets written in Visual Basic that can automate repetitive tasks. Although macro-based attacks have persisted, attackers have increasingly embraced the attack vector as a reliable fallback, especially as operating system and browser vulnerabilities become harder to find. Macro-based attacks have been instrumental in spreading ransomware. Microsoft is trying to block this risk completely and has decided to bring Application Guard to Office 365. Microsoft is offering a limited preview of Application Guard for the ProPlus version of Office 365. It's the same security feature that's in the Edge browser in Windows 10, which allows administrators to define trusted websites. Within Edge, untrusted websites are run in a Hyper-V container, which isolates them from the host operating system and hardware. If the website is malicious, it can't get outside the container to do damage.

Microsoft is trying to block this risk completely and has decided to bring Application Guard to Office 365.

Cyborg Ransomware (Fake 'Windows Update' Installs)

Transport Sector, NCIIPC

Ransomware has been widely used to attack different organizations and governments and has risen from 2017. A malicious spam campaign that informs victims that it contains a "critical Windows update" instead leads to the installation of Cyborg ransomware, they were able to access source code, which can be used to create malware variants. The ransomware uses email as a delivery platform. Another unique aspect is that the emails contain a two-sentence subject, "Install Latest Microsoft Windows Update now! Critical Microsoft Windows Update!" but the email body contains only one sentence. Typically, malicious emails include a longer, socially engineered message intended to lure victims into clicking malicious files. The fake update attachment has a ".jpg" file extension but is, in fact, an executable file sized around 28KB

A malicious spam campaign that informs victims it contains a Critical Windows update instead leads to the installation of Cyborg Ransomware.

with a randomized filename. The file is a malicious .NET downloader to deliver Cyborg ransomware to the system from Github. The attackers often use double extensions in order to trick users into opening a file," for example, "file.jpg.exe."

The fake Windows Update email has typical hallmarks of malicious spam. The suspicious subject line combined with "an executable attachment, not encased in an archive and with a .jpg extension". This is typical trick perform to spoof the file extension of an executable file to evade email gateways.

Though the Cyborg spam threat seemed to have abated, however, Cyber threat actors may modify the code and create versions for using it in targeted attacks.

References:

[1] https://threatpost.com/windows-update-cyborg-ransomware/150407/

[2] https://www.darkreading.com/threat-intelligence/attacker-mistake-botches-cyborg-ransomware-campaign/d/d-id/1336410

Cyber Threats in the Banking Industry

BFSI Sector, NCIIPC

Banking customers are moving away from using cash and cheque and relying more on electronic banking to complete transactions. In response to this shift, financial organizations continue to develop more web portals and mobile apps. Although these apps and portals are aimed at increasing convenience and enhancing the customer experience, they pose unique risks in terms of cyber security. A 2018 study by Accenture reviewed 30 major banking applications and found that all 30 had vulnerabilities ranging from insecure data storage to insecure authentication and code tampering. What's more, a similar study revealed that 85% of the tested web apps had flaws that would permit cyber-attacks against users. From lack of secure data storage to ineffective cryptography, there are a number of reasons why portals and banking apps pose a special threat:

- Lack of server security.
- Insecure or ineffective data storage.
- Data is not secured in the transport layer from server to client and/or from client to server.
- Data leakage on the user side.
- Inadequate authentication and authorization during user log-in.
- Client-side injection (e.g. the injection or execution of malicious code on the mobile device through the mobile app.

Cyber security breaches continue to grow in both frequency and sophistication for all industries, and the financial sector is particularly vulnerable.

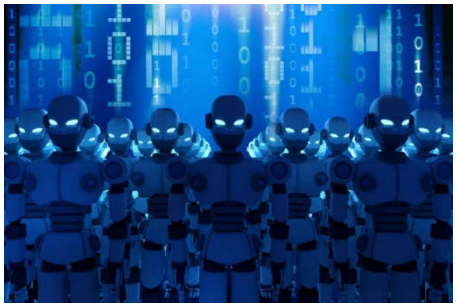
Solution for Secure Banking: The cyber risks that plague the banking industry are multiplied when you consider the vast number of users involved. The number of potentially insecure endpoints represents a candy store to cyber criminals. Recent statistics show online banking accounts for nearly 75 percent of all banking transactions, and this number is only expected to increase. The new Financial Services Sector Coordinating Council (FSSCC) profile is utilized by most major banking institutions along with other cyber security measures, although cybercrime continues to grow in sophistication.

References:

[1] https://attilasec.com/blog/banking-industry-cyber-threats/

[2] https://www.darkreading.com/threat-intelligence/attacker-mistake-botches-cyborg-ransomware-campaign/d/d-id/1336410

Malware Bytes



The attackers aim for the IoT vulnerabilities and target legacy devices which are too old to update but still in use.

Echobot Botnet casts a Wide Net with Raft of Exploit Additions

Source: https://threatpost.com

"Echobot", a variant of Mirai Internet of Things (IoT) botnet, has added 13 more vulnerability exploits to its bag of infiltration tricks. Network devices like Routers, Firewalls, IP cameras, server management utilities, programmable logic controller used in industrial environments, online payment system and even a Yatchcontrol web application are targeted. IoT botnets are bent on infecting connected devices in order to marshal their resources to carry out various nefarious activities, such as carrying out Distributed Denial-of-Service (DDoS) attacks. The attackers aim for the IoT vulnerabilities and target legacy devices which are too old to update but still in use and the newer vulnerabilities that are too recent to have a patch.

Malware Spitting Cash out of ATMs has spread across the World

Source: https://www.vice.com/

Jackpotting is a technique where cybercriminals use malware or a piece of hardware to trick an ATM into ejecting all of its cash, no stolen credit card required.

A joint investigation between Motherboard and the German broadcaster Bayerischer Rundfunk (BR) uncovered new details about the "jackpotting" attacks on ATMs in Germany in 2017 that saw thieves make off with more than a million Euros. ATM had been hacked with a malware called "Cutlet Maker" which has been designed to eject all of the money inside ATMs. Jackpotting is a technique where cybercriminals use malware or a piece of hardware to trick an ATM into ejecting all of its cash, no stolen credit card required. Hackers typically install the malware onto an ATM by physically opening a panel on the machine to reveal a USB port. In order to execute a jackpotting attack, one has to have access to the internal components of the ATM. ATM jackpotting is not limited to a single bank or ATM manufacturer.

DDoS Attacks, IoT Exploits: New Activity from Momentum Botnet

Source: https://blog.trendmicro.com

Researchers have found malware activity affecting devices running Linux. The analysis of retrieved malware samples revealed that these actions were connected to a botnet called Momentum. Momentum targets the Linux platform on various CPU architectures such as ARM, MIPS, Intel, Motorola 68020, and more. This malware opens a backdoor and accepts commands to conduct various DoS attacks against a given target. The backdoors Mirai, Kaiten, and Bashlite variants are being distributed by the Momentum botnet. This botnet spreads via exploiting multiple vulnerabilities on various routers and web services to download and execute shell scripts on the target device. The malware uses reflection and amplification methods that have a variety of targets: MEMCACHE, LDAP, DNS and Valve Source Engine. The malware spoofs source IP addresses to the various services running on public servers and provokes a flood of responses to the victim's address. Along with DoS attack, Momentum can also open a proxy on a port on a specified IP, disable or enable packeting from the client, and more.

The malware uses reflection and amplification methods that have a variety of targets: MEMCACHE, LDAP, DNS and Valve Source Engine.

WhatsApp Vulnerability Exploited through Malicious GIFs

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

A double-free vulnerability, CVE-2019-11932 was found in WhatsApp for Android versions below 2.19.244. Errors of such type can lead to memory leaks, crashes and arbitrary code execution. In this case, all it took to trigger the vulnerability and perform a Remote Code Execution (RCE) attack was the creation of a malicious GIF file. The bug can be triggered in two ways. The first one, which leads to local privilege escalation, requires a malicious application to already be installed on a target android device. The app then generates a malicious GIF file used to steal files from WhatsApp through the collection of library data. The second attack vector requires a user to be exposed to the GIF payload in WhatsApp as an attachment or through other channels. (If a GIF is sent directly through WhatsApp's Gallery Picker, however, the attack will fail.) Once the Gallery View is opened in the messaging application, the GIF file will be parsed twice and trigger a remote shell in the app, leading to successful RCE. Android versions 8.1 and 9.0 are exploitable, but older versions of the operating system -- Android 8.0 and below are not. The issue has been patched in WhatsApp version 2.19.244.

Android versions 8.1 and 9.0 are exploitable, but older versions of the operating system -- Android 8.0 and below -- are not.

Bluekeep Attacks are happening, but it's not a Worm

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

Image Source: https://blog.huntresslabs.com/keeping-up-with-bluekeep-d0676b976841

Impacts Windows 7, Windows Server 2008 R2, and Windows Server 2008

The BlueKeep (CVE-2019-0708) vulnerability in Microsoft RDP (Remote Desktop Protocol) service impacts Windows 7, Windows Server 2008 R2, and Windows Server 2008 operating systems. Patches have been available since mid-May 2019. A demo Bluekeep exploit released for the Metasploit penetration testing framework to help system administrators test vulnerable systems is being re-purposed by malicious actors. Security researchers have spotted mass-hacking campaign using the BlueKeep exploit; however, the exploit is not being used as a self-spreading worm. Instead, a hacker group has been using the demo BlueKeep exploit to hack into unpatched Windows systems and install a cryptocurrency miner. The person/group behind the recent attacks doesn't appear to have the know-how needed to modify the BlueKeep demo exploit released by the Metasploit team back in September, which is a good thing. However, some of their attacks have succeeded.

Exploit kits turn to Fileless Malware to evade Security Tools

Source: https://www.scmagazineuk.com/

Exploit kits, or EKs, are ready-built applications created by cyber-criminals and rented or sold to the highest bidder. Traffic from botnets or malicious ad campaigns is routed through the applications, selecting victims with specific configurations such as outdated browsers with known vulnerabilities to a landing page with the relevant exploit embedded within it. This then executes and installs the operator's choice of malware on the victim's machine. EK's are a rising threat, especially in browser-based drive-by attacks. The Internet Explorer is still under active attack, with new EK's is being developed. It has been observed that a growing number of EK's go for fileless attacks instead of the more traditional method where a payload on disk is dropped. This makes sample sharing more difficult and possibly increases infection rates by evading some security products.

Trickbot and Emotet Now Attacking the Healthcare Industry

Source: https://www.jdsupra.com/

Malwarebytes discovered a significant 82% spike in Trojan malware attacks on health care organizations in Q3 2019.

In a recent Cybercrime Tactics and Techniques Report focusing the health care industry, cybersecurity company Malwarebytes discovered a significant 82% spike in Trojan malware attacks on health care organizations in Q3 2019. Emotet and TrickBot, two especially sophisticated and dangerous forms of malware, were mostly responsible for this surge. Emotet is polymorphic, which makes it difficult for traditional antivirus solutions to detect. It worms its way through a network, generally using phishing

emails from compromised systems to spread as quickly as possible. Once enough computers are infected, it drops (install) other malicious programs, especially TrickBot, which has all sorts of modular, built-in tools to discover system information, compromise that system and steal data. Both of these Trojans are closely related to each other and presence of any one of these is a serious threat. Healthcare continues to be a prime target of scammers as the industry has known weaknesses, primarily due to the proliferation of connected but vulnerable devices.

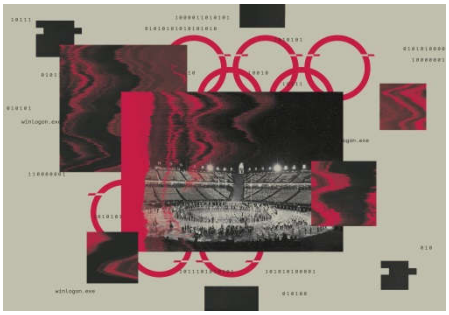
Healthcare continues to be a prime target of scammers as the industry has known weaknesses, primarily due to the proliferation of connected but vulnerable devices.

Learning

The Untold Story of the 2018 Olympics Cyberattack

Source: https://www.wired.com/, https://www.nytimes.com/

During the 2018 Winter Olympics opening ceremony the servers that formed the backbone of the Olympics' IT infrastructure were hit by malware. The malware attack not only shut down the Pyeongchang 2018 website, by taking out the Internet access but also shut down telecasts and prevented spectators from printing out tickets and attending the ceremony. The Olympic destroyer malware was attached to an email sent to Olympics staff. The attachment file on being opened ran a malicious macro script that planted a backdoor, offering the hackers the first foothold on the targeted network. The attack was stopped by a Korean security contractor, AhnLab, by creating an antivirus signature to vaccinate the network's thousands of PCs and servers against the malware that had infected them, a malicious file named winlogon.exe.



DOH Vs DOT Vs DNSSEC Vs DNSCurve/DNSCrypt

Director (NSAC), NCIIPC

DNS (Domain Name System) translates the domain names to IP addresses, which helps browsers to load web portal pages available on these addressees. DNS uses UDP for small queries and TCP for large queries like Zone Transfers over port 53. However, mentioned DNS queries and responses are in plain text/unencrypted, subject to MITM (Man-in-the-Middle) attack and privacy issues. IETF (Internet Engineering Task Force) Okayed two security protocols for DNS traffic encryption to overcome the problem of unencrypted DNS traffic as mentioned:

- DNS over TLS (Transport Security Layer) (DOT) which is an IEFTF RFC 7858 (Specification for DNS over Transport Layer Security) standard providing encryption between DNS client and server.
- DNS over HTTPS (DOH) which is IETF RFC 8484 (DNS queries over HTTPS) standard for providing encryption between DNS client and Server.

First malware attributed to DOH named Godlua which used the Confluence exploit (CVE-2019-3396) for infection was noticed in April 2019 by Qihoo 360, which has been tagged as DDOS bot which seems to evade passive DNS monitoring including other Cyber security apparatus due to difficulty in segregation of data at port 443.

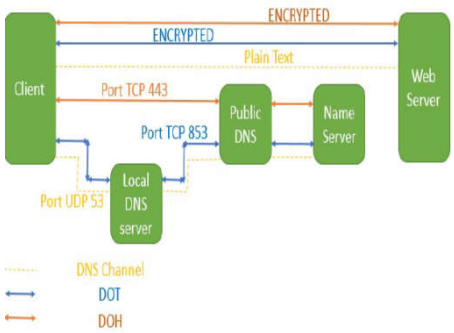


Figure 1

Though both the DOH and DOT provides the encryption for taking care of privacy and eavesdropping issues but there is another school of thoughts which argues that lot of metadata/information visà-vis DNS requests is revealed through IP address, SNI (Server Name Identification) and OSCP (Online Certificate Status Protocol) baring some information.

Recently Google and Firefox have been in the race for implementation of the DOH as a security protocol to which lot of security researchers and governments had reacted that it would be difficult to monitor the malicious activity/traffic (if implemented) including the issue of centralisation of entire DNS traffic with one ISP. Chrome will have Google DNS servers as request resolvers whereas Firefox is collaborating with Cloudfare for DNS resolves. Apart from DOH other alternatives are also available for DNS security as a unique solution or in solutions to be used in conjunction which will be discussed in the subsequent sections. It is also to be noted that some security researchers pointed that DNS is a part of control plane instead of data plane and will not affect privacy concerns, strengthening the belief that Network administrators should be able to monitor the same.

DOH: DOH is used over standard HTTPS port TCP port 443 for encrypting the DNS traffic. This removes the requirement of local Workstation level DNS resolver and local recursive resolver to query DNS records. Apps that currently support DOH come with hardcode DOH servers. DOH makes filtering and blocking more difficult as it is cumbersome to distinguish between normal web and DNS traffic, therefore blocking/filtering port 443 also means dropping HTTPS enabled web portal traffic. DOH also has capacity to combine with ToR systems for providing anonymity which has been already demonstrated by one of the ISP. On the downside of the technology, first malware attributed to DOH named Godlua which used the Confluence exploit (CVE-2019-3396) for infection was noticed in April 2019 by Qihoo 360, which has been tagged as DDoS bot which seems to evade passive DNS monitoring including other Cyber security apparatus due to difficulty in segregation of data at port 443.

DOT: DOT uses protocol and port separate from transmission by using TCP port 853 for performing name resolution. DOT can allow content blocking and filtering on TCP port 853 if DPI (Deep Packet Inspection) is enabled. BIND and Unbound supports local DNS resolver application in DOT.

Both DOH and DOT encrypts the traffic as compared to normal DNS request/responses which are in clear text and are subject to eavesdropping, however DOH omits the requirement of Local DNS server as depicted in Figure 1. Though both the DOH and DOT provides the encryption for taking care of privacy and eavesdropping issues but there is another school of thoughts which argues that lot of metadata/information vis-à-vis DNS requests is revealed by IP address, SNI (Server Name Identification) and OSCP (Online Certificate Status Protocol) baring some information.

DNSSESC: It thwarts DNS hijacking/spoofing by authenticating responses using public key cryptography which is getting legitimated through trusted digital certificates.

It creates the chain of trust but doesn't provide any encryption to the traffic which is still subject to MITM attack or privacy issues. It adds two basic features:

- Data Origin authentication, which verifies the originator.
- Data Integrity Protection, which verifies the integrity and ensure that data is not tempered in transit.

However, DNSSEC needs to be widely deployed in addition to be enabled by the network operators at recursive resolvers and Zone authentication level.

DNScurve/DNScrypt: These are the software solutions that encrypt the DNS request so that they are immune to the eavesdropping in channel between client and server, but were unable to garner the support because of the missing interest and support from larger commercial entities unlike DOH and DOT. DNSCurve ensure Confidentiality and Integrity for DNS requests/responses and DNS records including protection of Availability from forged DNS packets which may cause DoS/DDoS attack. DNSCrypt is aka SSL encryption which encrypts clear-text DNS traffic through lightweight software between client and DNS recursive name servers. DNScrypt is believed to prevent UDP based amplification attack and DNS spoofing because of requirement of length of questions for the requisite response and verification of the originated response.

Conclusion: DNS chain of trust and encryption is undoubtedly a requirement in the layered Cyber security framework, but at the same time governments across the world definitely have a humongous task in hand as far as monitoring and blocking is concerned which is sometimes vital to keep the malicious actors at the bay.

DOT as discussed in the above paragraphs, if implemented as a service can be deployed with DPI to localise the malicious monitoring and blocking along with DNSSEC which can add the missing trust element with chain of trust established through verified digital certificates.

DOT as discussed in the above paragraphs, if implemented as a service can be deployed with DPI to localise the malicious monitoring and blocking along with DNSSEC which can add the missing trust element with chain of trust established through verified digital certificates.

References:

[1] https://nciipc.gov.in/documents/Rules_procedures_new2018.pdf

[2] https://openrightsgroup.org

[3] https://arstechnica.com

[4] https://www.sans.org

[5] https://www.bleepingcomputer.com

[6] https://www.zdnet.com/

[7] https://blog.netlab.360.com/

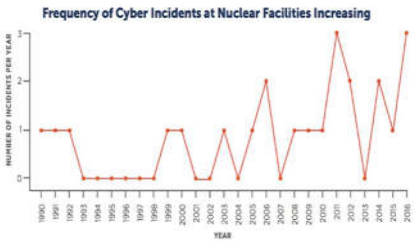
[8] https://www.icann.org/

[9] https://en.wikipedia.org/

[10] https://www.opendns.com/

Cyber Security in Nuclear Power Plants

S&PE Sector, NCIIPC



The number of publicly disclosed cyber incidents at nuclear facilities since 1990

Nuclear power plants stand among the most secure facilities in the country. Nuclear Power Plants are stand-alone and not connected to outside cyber network and Internet. Following practices have already been followed in Nuclear Power Plants:

- Digital Systems which contains the critical data are protected from being destructed or malicious use.
- These digital systems are not connected to the Internet. If pen-drives, CDs, or laptops are used to interface with plant equipment that have strictly monitored measures in place.
- Nuclear power plants have strong defences against an insider threat. Individuals who work with digital plant equipment are subject to increased security screening, cyber security training and behavioural observation.
- A cyber-attack could not prevent critical systems from performing their safety functions. The power plants should be shut down safely if necessary, even if there is a breach of cyber security.
- They are also designed to automatically disconnect from the power grid if there is a disturbance caused by a cyber-attack.

Any cyber-attack on the Nuclear Power Plant Control System is next to impossible but in this Age of Digital World, nothing can be said fully secured from cyber-attack. Nuclear plants have been addressing cyber-threats since nearly two decades. May be the cyber-attack can't be done from outside, but it can be done physically with the help of humans by carrying malware on a flash drive or portable computer, or by using vendor-required software updates that are already compromised, or let subcontractors in to work on various systems where they have access to the isolated network.

References:

[1] James Conca, "How Well Is The Nuclear Industry Protected From Cyber Threats?" 08 Nov 2019 [Online]. Available: https://www.forbes.com/sites/jamesconca/2019/11/08/how-well-is-the-nuclear-industry-protected-from-cyber-threats/#710c1ffb3497 [Accessed 16 Dec 2019]

[2] http://nuclearconnect.org/know-nuclear/talking-nuclear/nuclear-power-plant-cyber-security

Supply Chain Attacks

Source: https://docs.microsoft.com/

Supply chain attacks are an emerging threat that targets software developers and suppliers. Attackers look for unsecure network protocols, unsafe coding practices, and unprotected server infrastructures. They break in to change the source codes and hide the malware in build and update processes. Since, the software is built and released by trusted vendors, these apps and updates are signed and certified. In software supply chain attacks the vendors are usually unaware that their apps or updates are infected with malicious code when they are released to public. The malicious code then runs with the same trust and permissions as the app. Supply chain attacks can be pre-installed malware on devices, stolen code-sign using the identity of development company, compromised specialized code shipped into firmware or hardware components, and compromised software building tools or updated infrastructure. To protect against supply chain attacks, one must deploy strong code integrity policies to allow only authorized apps to run and use endpoint detection and response solutions that automatically detect and remediate suspicious activities. Also, software and developers should maintain a highly secure build and update infrastructure, build secure software updaters as part of the software development lifecycle and develop an incident response process for supply chain attacks.

Image Source: https://dzone.com/articles/how-to-reduce-the-impact-of-supply-chain-attacks-b

In software supply chain attacks the vendors are usually unaware that their apps or updates are infected with malicious code when they are released to public.

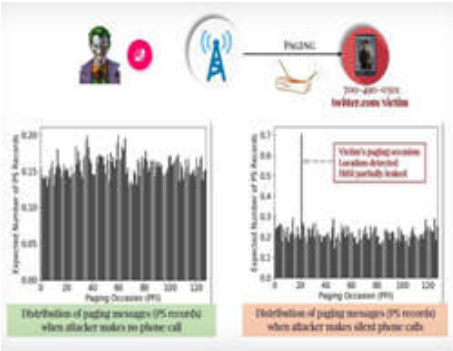
5G Threats: What are the Cyber Securities Implications?

Telecom Sector, NCIIPC

5G is no longer technology of the future, but a current reality. 5G will bring along a plethora of benefits, such as increased data speed, lower latency on network response time, and higher reliability. However, at the same time, new cyber security threats are likely to arise.

Security flaws in 5G enable various types of attacks: As pointed out by security researchers during Black Hat conference 2019, a security flaw in 5G allows Man-in-the-Middle (MiTM) attacks. It seems that security protocols and algorithm for 5G are now being ported from 4G standard and experts have discovered that this can allow device fingerprinting for targeted attacks and MiTM assaults. During the conference, researchers revealed that in 5G, as with 4G, the device capability information is sent to the base station before any security measures are applied to the connection. Basically, the traffic is encrypted from the endpoint to the base station, but since the device capabilities are sent before the encryption is applied, they can still be read in plain text. This enables multiple types of attack, like Mobile network mapping (MNmap), bidding down, and battery drain on the narrowband Internet of Things (NB IoT) devices.

5G will bring along a plethora of benefits, such as increased data speed, lower latency on network response time, and higher reliability.



This threat is capable of creating a map of devices connected to a certain network and list very specific details like device manufacturer, operating system, version, model, allowing them to precisely categorize a device as an Android or iOS, IoT or a phone, car modem, router, etc. In addition, this flaw opens the gate to targeted attacks against specific devices.

Researchers have also discovered three security flaws in both 4G and 5G, which can be exploited to intercept phone calls and track the locations of cell phone users. The first is Torpedo, which exploits a weakness in the paging protocol that carriers use to notify a phone before a call or text message comes through. Torpedo opens the door to two other attacks: Piercer, which the researchers say allows an attacker to determine an international mobile subscriber identity (IMSI), and the aptly named IMSI-Cracking attack, which can brute force an IMSI number in both 4G and 5G networks, where IMSI numbers are encrypted. The third flaw is Vulnerabilities in Signaling System 7, used by cell networks to route calls and messages across networks, are under active exploitation by hackers. The 5G technology could also lead to botnet attacks, which will spread at a much higher speed than the current networks allow it. Attackers could also use botnet to initiate Distributed-Denial-of-Service attacks.

Torpedo opens the door to two other attacks: Piercer, which the researchers say allows an attacker to determine an international mobile subscriber identity (IMSI), and the aptly named IMSI-Cracking attack

Conclusion: Extreme outcomes of security breaches are likely to happen due to 5G security flaws & prove to be both expensive and disastrous. This brings us to the most critical aspect that security experts should begin with, namely the fact that 5G networks must have, first of all, built-in security measures in place. But the first important step will remain to identify the security regulations that the 5G technology truly needs, coupled with strict cyber security rules and regulations imposed to 5G network providers.

References:

[1] https://heimdalsecurity.com/blog/5g-dangers-cybersecurity-implications/

[2] https://techcrunch.com/2019/02/24/new-4g-5g-security-flaws/

New Hack to Read Content of Password Protected PDF Files

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

PDFex technique includes two classes of attacks that take advantage of security flaws in a standard encryption protection built into the PDF. PDFex allows attackers to modify a protected PDF document, without having the corresponding password, in a way that when opened by someone with the right password, the file will automatically send out a copy of the decrypted content to a remote attacker-controlled server on the Internet.

The affected PDF viewers include popular software for Windows, macOS and Linux desktop OS such as: Adobe Acrobat, Okular, Foxit Reader, Evince, and Nitro Reader as well as PDF viewer that comes built into web browsers such as Firefox, Safari, Opera and Chrome. Security researchers have found that PDFex works because of the two major weaknesses in the PDF encryption. Partial Encryption that allows only strings and streams to be encrypted while objects defining the PDF document's structure remains unencrypted, this leaves an opportunity for attackers to easily manipulate the document structure and inject malicious payload into it; and Ciphertext Malleability in which PDF encryption uses the Cipher Block Chaining (CBC) encryption mode with no integrity checks, which can be exploited by attackers to create self-exfiltrating ciphertext parts.

The affected PDF viewers include popular software for Windows, macOS and Linux desktop OS such as: Adobe Acrobat, Okular, Foxit Reader, Evince, and Nitro Reader as well as PDF viewer that comes built into web browsers such as Firefox, Safari, Opera and Chrome.

Vulnerability Watch

Any Fingerprint can Unlock Samsung Galaxy S10 phone

Source: https://gizmodo.com/

A flaw had been identified in Samsung Galaxy S10 where any fingerprint could unlock the device. According to Samsung, the source of the problem is an issue with the device's ultrasonic fingerprint sensor that causes the phone to mistakenly recognize 3-dimensional patterns in certain silicone covers and screens protectors themselves as the user's fingerprint. Company is going to release a patch for the issue.

Image Source: https://www.firstpost.com/

Critical flaws in VNC threaten Industrial Environments

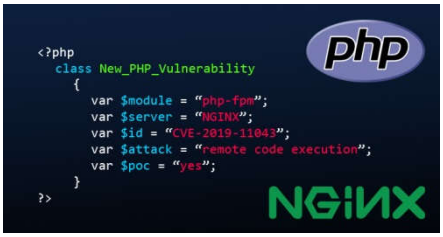
Source: https://threatpost.com/critical-flaws-vnc-industrial/150568/

Several vulnerabilities have been identified in remote access system Virtual Network Computing (VNC) - LibVNC, UltraVNC, TightVNC1.X and TurboVNC. Many of these vulnerabilities are critical and some of which could result in Remote Code Execution (RCE). Kaspersky researchers found vulnerabilities in both the client and the server-side of the system. Patches for affected products have been issued and TightVNC has discontinued the development of the TightVNC 1.X line and considers it end of life, so the bugs won't be patched.

PHP flaw could let attacker hack sites running on Nginx Servers

Source: https://thehackernews.com/, https://nvd.nist.gov/

In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 running on NGINX with PHP-FPM enabled could be vulnerable to the remote code execution vulnerability (CVE-2019-11043).



A website is vulnerable, if:

- NGINX is configured to forward PHP pages requests to PHP-FPM processor, fastcgi_split_path_info directive is present in the configuration and includes a regular expression beginning with a '^' symbol and ending with a '$' symbol,
- PATH_INFO variable is defined with fastcgi_param directive,
- There are no checks like try_files $uri =404 or if (-f $uri) to determine whether a file exists or not.

The patch for PHP7's FPM flaw has been released.

Design flaw could open Bluetooth devices to Hacking

Source: https://www.eurekalert.org/

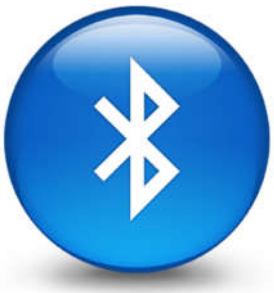


Image Source: https://cyberops.in

A new research has found that Mobile apps that work with Bluetooth devices have an inherent design flaw which makes them vulnerable to hacking. The problem lies in the way Bluetooth Low Energy devices communicate with the mobile apps that control them. Security researcher Lin said that it was in the initial app-level authentication, the initial pairing of the phone app with the device, where the vulnerability existed. If app developers tightened defenses in that initial authentication the problem could be resolved.

TPM-FAIL Impact TPM Chips in Desktops, Laptops and Servers

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

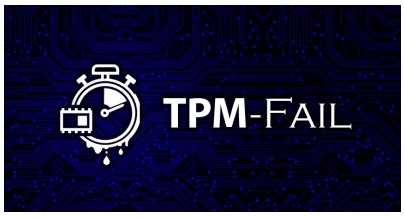


Image Source: https://thehackernews.com/

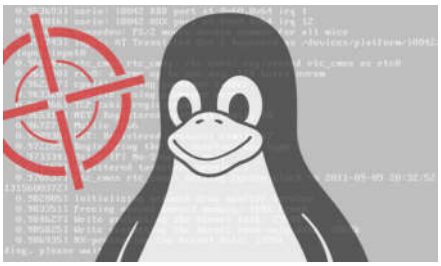
Trusted Platform Module (TPM) is chips added to motherboard were CPU stores and manages sensitive information such as cryptographic keys. With the evolution of hardware ecosystem software-based solution were developed in the form of firmware-based TPMs -- also known as fTPMs. Two vulnerabilities collectively known as TPM-FAIL could allow an attacker to retrieve cryptographic keys stored inside TPMs. The first vulnerability is CVE-2019-11090 and impacts Intel's Platform Trust Technology (PTT). Intel PTT is Intel's fTPM software-based TPM solution and is widely used on servers, desktops, and laptops, being supported on all Intel CPUs released since 2013, starting with the Haswell generation. The second is CVE-2019-16863 and impacts the ST33 TPM chip made by ST Microelectronics; it is hardware-enforced TPM. Of the two, the issue impacting Intel's fTPM solution is considered the most dangerous, as it could be exploited remotely. Intel has released firmware updates for the Intel PTT and STMicroelectronics prepared a new iteration of the ST33 chip.

Four-Year-Old Linux Wi-Fi bug allows System Compromise

Source: https://threatpost.com/

Buffer overflow vulnerability (CVE-2019-17666) exists in the

"rtlwifi" driver, which is a software component used to allow certain Realtek Wi-Fi modules, used in Linux devices, to communicate with the Linux operating system. The vulnerable piece of the rtlwifi driver is a feature called the Notice of Absence protocol. This protocol helps devices autonomously power down their radio to save energy. The flaw exists in how the driver handles Notice of Absence packets: It does not check certain packets for a compatible length, so an attacker could add specific information elements that would cause the system to crash. Versions through 5.3.6 of the Linux kernel operating system are impacted.



Security App

GitHub Security Lab: CodeQL find the Unknown Vulnerability

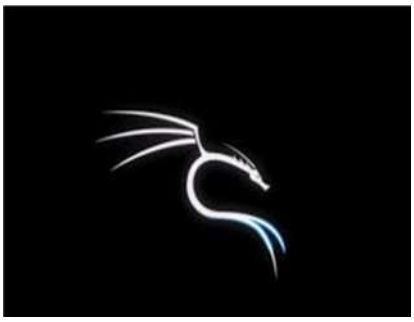
Source: https://github.blog/

GitHub Security Lab made its code analysis engine CodeQL freely available to find vulnerabilities in open source code. CodeQL is a tool used to perform semantic analysis of code. GitHub Security Lab will help to identify and report vulnerabilities in open source software, while maintainers and developers use GitHub to create fixes, coordinate disclosure, and update dependent projects to a fixed version. CodeQL allows to quickly performing variant analysis to find previously unknown security vulnerabilities. It treats code as data allowing individual to write custom queries to explore their code. CodeQL ships with extensive libraries to perform control and data flow analysis, taint tracking and explore known threat models without having to worry about low-level language concepts and compiler specifies. Supported languages include C/C++, C#, Java, JavaScript, Python and more.

Kali Linux 2019.4 includes new Undercover Mode

Source: https://www.helpnetsecurity.com/2019/11/27/kali-linux-2019-4/

Offensive Security, maintainers of the popular Kali Linux open source project, released Kali Linux 2019.4, the latest iteration of the Kali Linux penetration testing platform. The new release includes several new features including a new default desktop environment, a new theme and a new undercover mode for pentesters doing assessment work in public places. The most noteworthy aspect of the 2019.4 release is Kali's move from the Gnome environment to Xfce. The new release enables pentesters doing work in public places to change Kali theme to look like a default Windows installation by executing a script. That's way, pentesters can work a bit more incognito. Pentesters can switch back to Kali theme by running the script again.



The new release enables pentesters doing work in public places to change Kali theme to look like a default Windows installation by executing a script

Image Source: https://www.eletimes.com

Microsoft Cloud Security Solutions provide Comprehensive Cross Cloud Protection

Source: https://www.microsoft.com/

Many organizations operate a cross-cloud environment that complicates security. A fragmented view of cloud environment limits opportunities to holistically improve security posture which leads to missed threats and SecOps burnout. To address these challenges, Microsoft provides a set of comprehensive Cloud Security solutions to protect every layer of the cloud. Microsoft Cloud Security solutions can help to realize integrated visibility and protection across clouds with Cloud Security Posture Management and Cloud Workload Protection Platform solutions. It also helps to develop and secure custom apps in the cloud with Application Security services. It monitors and controls user activities and data across all apps with its leading Cloud Access Security Broker (CASB). Microsoft's Azure Security Center continuously monitors cross-cloud resources such as virtual machines, networks, applications, and data services. Microsoft Application Security services offer operations and development tools that help in identifying potential threats before deploying application in production. Microsoft Cloud App Security provides rich visibility into shadow IT and enables to identify and remediate cloud native attacks.

NCIIPC Initiatives

DG, NCIIPC at the National Workshop on Cyber Security for Critical Infrastructure

National Workshop on Cyber Security

Dr Ajeet Bajpai, DG, NCIIPC was 'Guest of Honour' at the two days National Workshop on Cyber Security for Critical Infrastructure, organized by Society for Electronic Transactions and Security (SETS) and C-DAC on 27th September 2019. Main objective of SETS is knowledge creation in cryptology, hardware security and network security to meet specific long-term and short-term needs of the Nation.

Two days Cyber Security awareness program for Power Sector

Cyber Security Awareness Program at THDC Rishikesh & Tehri

NCIIPC organized two days Cyber Security awareness program for Power Sector at Tehri Hydro Power Corporation Limited (THDC) at Rishikesh and Tehri on 25th & 27th September 2019 respectively. Director NCIIPC discussed about the roles and responsibilities of NCIIPC and basics of cyber security hygiene.

NCIIPC at 29th IISM Annual Global Conclave

International Institute of Security and Safety Management (IISSM) organized 29th Annual Global Conclave in Bangalore on 14-15 November 2019. The theme for the Conclave was 'New Paradigms for Loss Prevention in the Digital Era.' Col Pradeep Bhat (Retd), Consultant, NCIIPC moderated the panel discussion on Artificial Intelligence and Business Security: Opportunities and Drivers for Future Growth.

Col Pradeep Bhat (Retd), Consultant, NCIIPC at 29th IISM Global Conclave

A Two Day DTF Event for Critical Sectors in South Zone

NCIIPC along with Information Sharing and Analysis Centre (ISAC) organized a two day Defend the Flag (DTF) event for various Critical Sectors of South Zone on 14th and 15th November, 2019.

NCIIPC at IDRBT-CISO Forum Meet

Shri Sanjeev Chawla, DDG, NCIIPC delivered talk on Critical Information Infrastructure for Banking Sector during the IDRBT-CISO Forum (Indian Banking and Financial Sector- Chief Information Security Officers) meet on 21st November 2019 at Gurugram. IDRBT-CISO forum provides a platform for sharing latest security technologies, day-to-day problems in implementing security in banks and means to continuously upgrade the security posture of Banks.

Shri Sanjeev Chawla, DDG, NCIIPC at the IDRBT- CISO Forum Meet

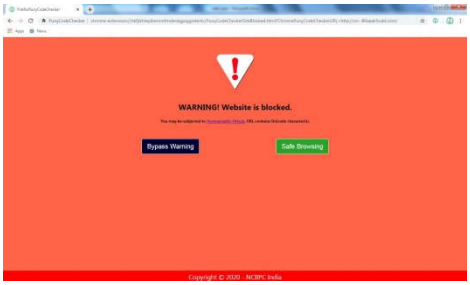
One day Cyber Security Workshop for Petroleum & Natural Gas Sector

GAIL (India) Limited organized 1st Cyber Security meet to create awareness among the members from Petroleum & Natural Gas Sectors like IOCL, BPCL, HPCL etc about the Cyber Threats in Information & Data Security at Jubilee Tower, Noida, Uttar Pradesh on 26th November 2019. Sectoral Coordinator shared Role of NCIIPC along with best practices to mitigate cyber threats and discussed OT technology challenges.

Cyber Security Workshop for Petroleum & Natural Gas Sector

Establishment of NCIIPC Zonal Office (West)

NCIIPC commenced operation from its Zonal Office (West) located at IIT Bombay Research Park on 05th December 2019. This is aimed to reach out to all its stakeholders in West Zone.



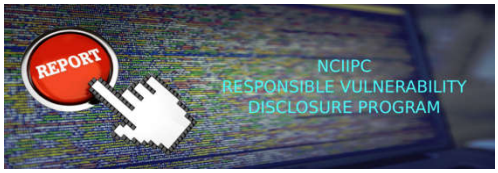
'PunyCodeChecker' plugin warns users before visiting a website with non-ASCII characters.

Browser Extension for Protection from Homograph Attack

https://addons.mozilla.org/en-US/firefox/addon/punycodechecker/

NCIIPC has developed browser-extension (plugin) for both Mozilla and Chrome desktop users named as the 'PunyCodeChecker'. This is aimed to protect Internet users from Homograph Attack. Homograph attack is almost undetectable by any modern-day browsers and mostly used for phishing purposes that are aimed to trick the most careful users on the Internet. It exploits the fact that many different characters look alike in naked eye (i.e. they are homographs).

To make this distinction easy, 'PunyCodeChecker' plugin warns users before visiting a website with non-ASCII characters. One can though navigate to the website by bypassing the warning or may proceed with safe browsing option. Download and install 'PunyCodeChecker' for Mozilla and Firefox to remain safe.



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

NCIIPC Responsible Vulnerability Disclosure Program

https://nciipc.gov.in/RVDP.html

The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in Nation's Critical Information Infrastructure. NCIIPC acknowledges the following top 15 researchers for their contributions during Q4-2019 towards disclosure of vulnerabilities for protection of National Critical Information Infrastructure:

- Akash Yadav
- Sagar Banwa
- Kirankumar Subuddi
- Badal Sardhara
- Deepak Kumar Bharti
- Abhimanyu Raj
- Andy Hook
- Animesh Gupta
- Roshan Chauhan
- Kaustubh Rasam
- Tolesh Kumar Jangid
- Mohit Khemchandani
- Shailesh Kumar
- Ankit Sharma
- Tushar Vaidya

Mobile Security

StrandHogg: Spoofing an App UI

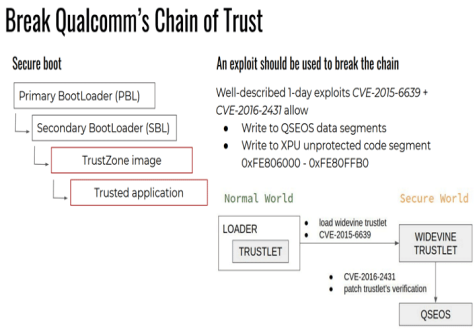
Source: https://thehackernews.com/, https://promon.co/

Researchers at Norwegian security firm Promon have discovered a new vulnerability in Android operating system dubbed as 'StrandHogg' which abuses taskAffinity and allowTaskReparenting attribute of an activity to match the packageName of any third-party app and launches a spoofing UI of that app. Masquerading an app, it steals users' credentials and can also ask for sensitive device permissions. According to mobile security firm Lookout, 36 malicious apps have already been found to be exploiting this vulnerability. This vulnerability works with all versions of Android including Android 10 and can be exploited without root access.

Vulnerability in Qualcomm Chipsets

Source: https://thehackernews.com, https://research.checkpoint.com

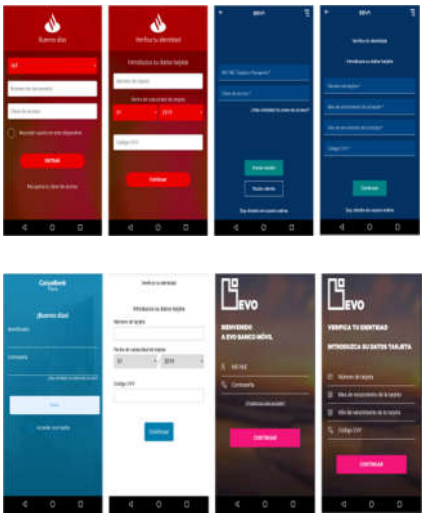
Android smartphones and tablets from Samsung, Motorola, LG running on Qualcomm chipsets are facing security threats due to vulnerability lying in Qualcomm's Secure Execution Environment (QSEE) which is an implementation of Trusted Execution Environment (TEE) based on ARM TrustZone technology. QSEE contains sensitive information such as private encryption keys, passwords, and credit and debit card credentials. Cybersecurity firm CheckPoint has implemented a custom-made fuzzing tool on reverse-engineered QSEE to find vulnerabilities such as dxhdcp2 (LVE-SMP-190005), sec_store (SVE-2019-13952), authnr (SVE-2019-13949), esecomm (SVE-2019-13950), kmota (CVE-2019-10574), tzpr25 (Samsung) and prov (Motorola). This leads to leakages of device data, device rooting, bootlocker unlocking and execution of undetectable APT.



ai.type Keyboard Making Unauthorized Transactions

Source: https://www.welivesecurity.com/

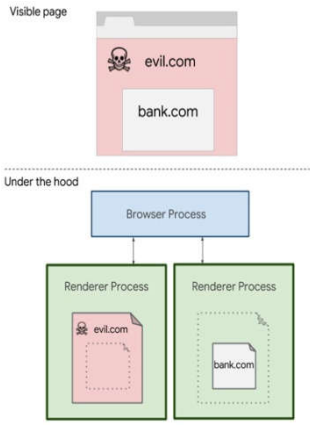
'ai.type Free Emoji Keyboard' with over 40 million downloads has been accused of attempting to make over 14 million unauthorized transactions from 110,000 unique devices across 13 countries, mainly from North Africa and South America. In the background, the app automatically performs clicks using software development kits (SDKs) with "obfuscated hard-coded links back to advertising trackers" which leads to users' subscribing to premium services unknowingly. The app was taken down from Google Play Store in June but still exists largely in alternative Android marketplaces. Last year, the developers of ai.type were accused of exposing 31 million users' personal data on an unprotected server.



Ginp: A Banking Malware from Anubis

Source: https://www.threatfabric.com/

According to Threatfabric, there is a new banking malware in town known as 'Ginp' which takes its cue from famous Trojan 'Anubis'. Though it is built from scratch with regular updates, the fifth or latest one includes code from Anubis. Initially, dubbed as 'Google Play Verificator' app, Ginp used to steal SMSs by masquerading. In August 2019, posing as 'Adobe Flash Player' apps, it included some banking-specific features focusing on Spanish banks like Caixa bank, Bankinter, Bankia, BBVA, EVO Banko, Kutxabank and Santander. The malware first shows overlay screens of banks to the users and then steal their login credentials followed by credit card details and send it to a C2 server. Its main focus is on overlay attacks, SMS control and contact list harvesting. It also asks for Accessibility Service Privilege, and once granted, it grants itself additional dynamic permissions. By analyzing its code, Ginp is expected to be equipped with more advanced features like back-connect proxy, screen-streaming and RAT in near future.



Site Isolation for Chrome on Android

Source: https://thehackernews.com/

'Site Isolation' has now been added to Google Chrome on Android. It was previously available to Chrome desktop users only. With the help of this additional security feature, different sites are being rendered in their separate sandboxes on browser. It prevents cross-site data stealing like theft of sensitive data, authentication cookies, stored passwords, network data, stored permissions which in turn can stop Spectre and Meltdown like side-channel vulnerabilities. As a performance trade-off, the security feature works only with sites having login using passwords. Users are advised to update their Chrome to version 77 for Android.

App Defense Alliance for Google Play Store

Source: https://security.googleblog.com/

Google has formed an 'App Defense Alliance' with ESET, Lookout and Zimperium for protection of users in Google Play Store. With the help of each partner's scanning engines which includes a combination of machine learning and static/ dynamic analysis to detect abusive behaviour, Google Play Protection Detection system will generate new app risk intelligence before publishing any app to play store. This will prevent potentially harmful apps going live in store which can harm Android users.

Upcoming Events - Global

January 2020

- FS-ISAC Cyber-Range Exercise 2020, Toronto — 15 Jan
- S4X20, Florida — 20-23 Jan
- Cyber Security for Critical Assets (CS4CA) MENA, Dubai — 20-21 Jan
- Common Information Model, Amsterdam — 21-23 Jan
- Data and the Future of Financial Services, London — 22 Jan
- Annual PCI London Summit, London — 23 Jan
- NextGen SCADA, Berlin — 27-31 Jan
- DACH Strategy Forum Cyber and Information Security, Munich — 28-29 Jan

February 2020

- MANUSEC Europe, Munich — 4-5 Feb
- IT-Defense 2020, Bonn, Germany — 5-7 Feb
- Global Cyber Security in Healthcare & Pharma Summit, London — 6-7 Feb
- Payments Summit, Salt Lake City — 24-27 Feb
- RSA Conference USA, San Francisco — 24-28 Feb
- TackleCon, San Francisco — 26 Feb
- BSides Tampa, Florida — 29 Feb

March 2020

- Cyber Intelligence Asia, Kuala Lumpur — 10 Mar
- Nordic Cyber Series, Copenhagen, Denmark — 10 Mar
- Africa ICS Cybersecurity Conference and Expo, Nairobi, Kenya — 10-13 Mar
- InfoSec Connect, San Diego — 15-17 Mar
- Cyber Security And Cloud Expo Global 2020, London — 17 Mar
- 2020 Fraud Summit, New York — 18 Mar
- CyberCon Power & Utilities CISO Summit and Cybersecurity Conference, Anaheim — 30 Mar

April 2020

- Know Identity Las Vegas, Las Vegas — 5-8 Apr
- OFFZONE 2020, Moscow — 16-17 Apr
- Cyber Security & Fraud Summit, Chicago — 21 Apr

JANUARY 2020

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	

FEBRUARY 2020

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

- ICS Cyber Security Conference 2020, London — 28 Apr
- Critical Infrastructure Protection and Resilience Americas, New Orleans — 28-30 Apr
- Cyber Security of Critical Infrastructure (CYSEC), Dubrovnik, Croatia — 29-30 Apr

MARCH 2020

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				

APRIL 2020

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		

Upcoming Events - India

- COMSNETS 2020, Bengaluru — 7 Jan
- United Conference on Cyber Space (UNITEDCON2020), New Delhi — 14 Jan
- GRC Meet, New Delhi — 17 Jan
- 3rd Edition CRO Leadership Summit & Awards 2020, Mumbai — 23 Jan
- Internet of Things India Expo, New Delhi — 19-21 Feb
- Third ISEA Conference on Security and Privacy 2020, Guwahati — 27 Feb
- Nullcon 2020, Goa — 3-7 Mar
- Cyber Security Summit, Bengaluru — 6 Mar
- Gartner IT Infrastructure, Operations & Cloud Strategies Conference 2020, Mumbai — 14 May

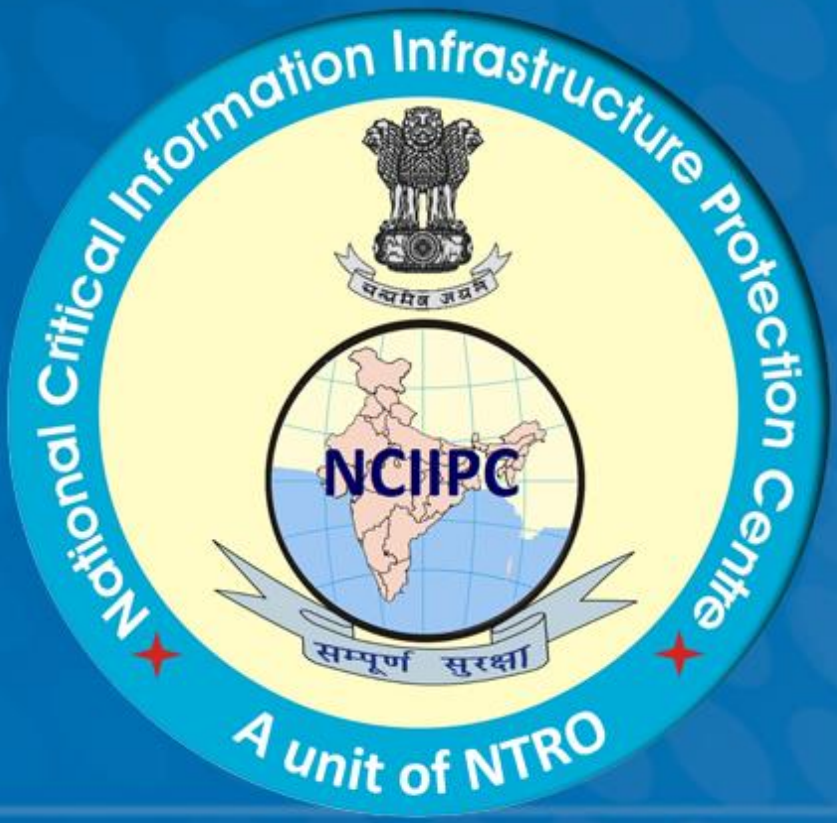
General Help helpdesk1@nciipc.gov.in
helpdesk2@nciipc.gov.in

Incident Reporting : ir@nciipc.gov.in

Vulnerability Disclosure : rvdp@nciipc.gov.in

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

Notes



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.