NEWSLETTER

January 2018

National Critical Information Infrastructure Protection Centre

VOLUME 2 ISSUE 1

@NCIIPC

NCIIPC Newsletter

January 2018

Inside This Issue

India hosted the 5th Global Conference on Cyber Space (GCCS 2017) from 23-24 Nov 2017 at New Delhi. It was attended by more than 3500 participants from over 135 countries.

Message from the NCIIPC Desk

NCIIPC wishes all of its stakeholders a happy and secure 2018. 2017 has been an eventful year in the domain of cyber security. There is a growing awareness of cyber hygiene in India and globally. The Digital India initiative, thrust towards digital economy and e-governance posed new threats and challenges for different stakeholders in the country.

The increase in ransomware attacks and sophistication of weaponized malware created a global urgency for immediate implementation of cyber security practices. WannaCry, Petya, NotPetya gained immense notoriety. Tackling such menace calls for a multi-stakeholder approach transcending organisational, national and international borders. There is an urgent need for regulating cyber space and formulating a Global Treaty.

India hosted the 5th Global Conference on Cyber Space (GCCS 2017) from 23-24 Nov 2017 at New Delhi. It was attended by more than 3500 participants from over 135 countries. The Finals of the Hackathon Event was hosted by National Critical Information Infrastructure Protection Centre (NCIIPC).

India became member of the Meridian community by participating in the 13th Meridian Annual Conference held in Oslo, Norway on 24-25 October 2017. The Meridian Process aims to exchange ideas and initiate actions for the cooperation of governmental bodies on Critical Information Infrastructure Protection (CIIP) issues globally. The Indian delegation was led by Dr Ajeet Bajpai, DG, NCIIPC who presented the 'Challenges in Critical Information Infrastructure Protection'.

NCIIPC organised cyber security sensitisation workshops at Chandigarh and Imphal in collaboration with the State Governments of Punjab and Manipur respectively. NCIIPC continues its endeavour to facilitate safe, secure and resilient information infrastructure for critical sectors in the Nation.

The NCIIPC Newsletter initiative completes a year in January, 2018. We thank all our readers for their encouragement and feedback. Kindly keep mailing your suggestions and contributions at newsletter@nciipc.gov.in

News Snippets - National

Prime Minister Inaugurates the 5th Global Conference on Cyberspace

Source: http://pib.nic.in/

GCCS 2017
GLOBAL CONFERENCE ON CYBERSPACE

Sh. Narendra Modi, Hon'ble Prime Minister of India inaugurated the Global Conference on Cyberspace (GCCS) 2017 in the Capital on 23rd November in the presence of His Excellency, Mr. Ranil Wickramasinghe, Prime Minister of Sri Lanka, Sh. Ravi Shankar Prasad, Hon'ble Minister for Electronics & IT, Secretary General of International Telecommunication Union, Mr. Houlin Zhao amongst other dignitaries. Themed on Cyber4All: A Secure and Inclusive Cyberspace for Sustainable Development, is the 5th edition of GCCS wherein international leaders, policymakers, industry experts, think tanks and cyber experts gathered to deliberate on issues and challenges for optimally using cyber space. In his inaugural address, Sh. Narendra Modi, said, "*The quest for an open and accessible Internet often leads to vulnerability. Stories of hacking and defacement of websites are the tip of an iceberg. They suggest that cyber attacks are a significant threat, especially in the democratic world. We need to ensure that vulnerable sections of our society do not fall prey to the evil designs of cyber criminals. Alertness towards cyber-security concerns, should become a way of life. One of the major focus areas should be the training of well-equipped and capable professionals to counter cyber threats.*" "*On a related note, nations must also take responsibility to ensure that the digital space does not become a playground for the dark forces of terrorism and radicalization.*" added Sh. Narendra Modi. The Prime Minister also felicitated the winners of the Global Cyber Challenge called 'Peace-a-thon' and 'Capture the Flag' (CTF) contest. Winners were declared following a 36-hour challenge in the Grand Finale of the Hackathon, with hundreds of teams from across India and other countries like the USA, Canada, France, Argentina, Australia and Algeria turned up to showcasing their talent and competing. It was conducted with the Ministry of Electronics and Information Technology, National Critical Information Infrastructure Protection Centre (NCIIPC), MyGov, Cyber Peace Foundation and Policy Perspectives Foundation as collaborators. Incepted in 2011 in London, 2nd GCCS was held in 2012 in Budapest, the 3rd edition of GCCS was held in 2013 in Seoul, the 4th version of GCCS 2015 was held in The Hague, Netherlands, which saw participation from 97 countries. The GCCS logo symbol for the 5th edition takes inspiration from Indian philosophy and the Sanskrit term '*bindu*', meaning a small 'dot' or a 'point'. The logo is contemporary and modern, but completely Indian in origin as well as in the vibrant colour palettes.

Prime Minister Narendra Modi with his Sri Lankan counterpart Ranil Wickremesinghe (right) and IT minister Ravi Shankar Prasad (left) in GCCS 2017. Photo: AP

> *"Cyber attacks are a significant threat, especially in the democratic world. We need to ensure that vulnerable sections of our society do not fall prey to the evil designs of cyber criminals. Alertness towards cyber-security concerns, should become a way of life." – The PM*

Info Sec professionals get ready for the Operational Technology Capture the Flag contest hosted at NCIIPC

India-New Zealand Cyber Dialogue

Source: http://mea.gov.in/

The 1st India-New Zealand Cyber Dialogue was held in New Delhi on November 27, 2017. The Indian Delegation was led by Mr. Sanjay Kumar Verma, Additional Secretary, Ministry of External Affairs. It included representatives from the Ministry of Electronics and IT, National Security Council Secretariat, Central Bureau of Investigation, Department of Telecommunication, National Critical Information Infrastructure Protection Centre (NCIIPC), while the New Zealand delegation was led by Mr. Paul Ash, Director of the National Cyber Policy Office, Department of Prime Minister and Cabinet who was accompanied by representatives from the International Security & Disarmament Division, Ministry of Foreign Affairs and Trade, and officials from its High Commission in New Delhi. India and New Zealand reaffirmed their commitment to an open, free, secure, stable, peaceful and accessible cyberspace, enabling economic growth and innovation. Both sides recognised the multi-stakeholder approach as a core element in their cyber policy. In particular, both sides reaffirmed that the existing principles of international law are applicable in cyberspace and that there was a need to continue and deepen deliberations on the applicability of International Law to cyberspace and set norms of responsible behaviour of states. They also emphasised the significance of various regional, international and multilateral initiatives, particularly UN facilitated initiatives, to continue the debate on these issues as well as on cyber capacity building. The two countries also agreed that the bilateral cyber dialogue provided a strong foundation for existing and future cooperation. Areas of discussion included domestic cyber policy landscape, cyber threats and mitigation, new technologies, mechanism on bilateral cooperation and possible cooperation at various international fora and regional fora. Both sides shared the view that they will deepen the dialogues at various levels. Both sides agreed to hold the next India-New Zealand Cyber dialogue in New Zealand in 2018.

India and New Zealand reaffirmed their commitment to an open, free, secure, stable, peaceful and accessible cyberspace, enabling economic growth and innovation.

Companies Must Work More Closely With CERT-In and NCIIPC

Source: https://timesofindia.indiatimes.com/

National Cyber Security Coordinator (NCSC), Dr. Gulshan Rai

Companies operating in cyber security solutions and services domain must work more closely with central organisations like Indian Computer Emergency Response Team and National Critical Information Infrastructure Protection Centre to secure the entire digital ecosystem across India, National Cyber Security Coordinator, Dr. Gulshan Rai said at an event co-hosted by ASSOCHAM and Kaspersky in New Delhi.

Inaugurating ASSOCHAM-Kaspersky Cyber Resilience Summit, Rai stated that cyber security companies need to shun their usual practice of being hesitant in sharing sensitive data with government organisations through enhanced mutual co-operation and trust. "*They may not share it publicly but certain data highlighting the offending or malicious IPs (internet protocol address) they must share it with central organisations so that country at large can benefit and the entire digital ecosystem can be prevented*," he said. The National Cyber Security Coordinator termed machine learning and artificial intelligence as a double-edged technology which while helps in identifying the background processes but also provides hackers with information to breach the systems. Highlighting the need to follow processes and skill to achieve high resilience in the cyber world, Dr Rai said, "*If we follow the processes and properly interpret the results of artificial intelligence or machine learning we would be able to enhance the resilience of our digital systems and minimise the impact of many cyber attacks.*"

> *"They may not share it publicly but certain data highlighting the offending or malicious IPs (internet protocol address) they must share it with central organisations so that country at large can benefit and the entire digital ecosystem can be prevented," - NCSC*

A Testing Facility for Power Equipment before its Installation

Source: http://www.deccanherald.com/

To prevent cyber-attacks on electricity network, the ministry of power is planning to set up a testing facility for power equipment before its installation. The Central Electricity Authority is working to amend the regulations to ensure only tested equipment be installed in the network mainly in the distribution sector. The government is also working on stringent regulations to check imported equipment to ensure it is free from malware. To share and analyse various cyber security incidents in the power sector, Information Sharing and Analysis Centre (ISAC-Power) centre has been set up. The ISAC-Power will be the common central information resource pooling and sharing platform. For better power distribution and management, several states are implementing Supervisory Control and Data Acquisition Systems (SCADA). Recently the domestic electrical equipment industry raised concerns over some specific foreign companies bagging the contract for installation of SCADA for power distribution in many Indian states.

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF POWER

> *The Central Electricity Authority is working to amend the regulations to ensure only tested equipment be installed in the network mainly in the distribution sector.*

News Snippets - International

Hackers Stole the Personal Data of 145.5 million Americans

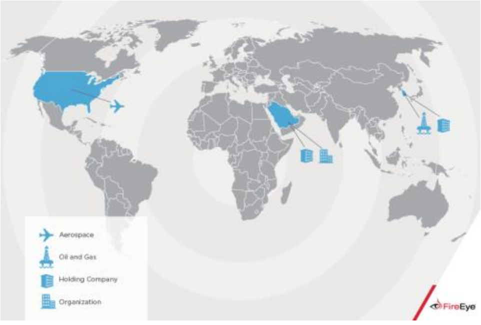
Photo: (Mike Stewart/AP)

Source: https://motherboard.vice.com/

On September 7, Equifax, the largest credit reporting agency in the United States, disclosed the massive hack of its internal systems. The firm, which, ironically, sells services to monitor data breaches, revealed hackers had stolen the sensitive personal data of 145.5 million Americans, including social security numbers, names, home addresses, and driver's license numbers. Given that bank and other financial institutions rely on Equifax's data to verify the identity of potential customers seeking credit; this was a massive, damaging hack not only to the 145.5 million victims, but the whole US economy. Equifax has publicly blamed the breach on an unpatched vulnerability in the web application software Apache Struts and on one employee who failed to identify it and patch it on a specific consumer dispute portal. "*Being a trusted steward of data is vital to the mission of Equifax*," the company's former CEO Richard Smith, who resigned in the wake of the data breach, told lawmakers during a hearing on October 4.

This was a massive, damaging hack not only to the 145.5 million victims, but the whole US economy.

A Cyber-espionage Campaign Targeting Aerospace, Petrochemical and Energy Sector Firms



Scope of APT33 Targeting
Source: www.fireeye.com

Source: https://threatpost.com/

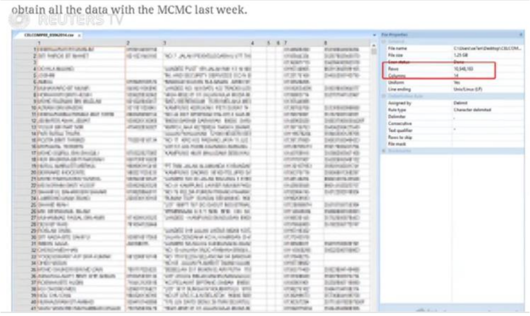
The APT33 group is believed to be behind a cyber-espionage campaign targeting aerospace, petrochemical and energy sector firms located in the United States, Saudi Arabia and South Korea. The group's latest attack leverages a dropper called DropShot that is tied to the StoneDrill wiper malware (a variant of the infamous Shamoon 2), according to a report released by FireEye. The malware is being distributed via spear phishing campaigns that include advertisements for jobs at Saudi Arabian aviation companies and Western organisations. Emails include recruitment themed lures that contain links to malicious HTML application (.hta) files. "*The .hta files contained job descriptions and links to legitimate job postings on popular employment websites that would be relevant to the targeted individuals*," researchers said. "*Unbeknownst to the user, the .hta file also contained embedded code that automatically downloaded a custom APT33 backdoor (TurnedUp).*" Links in emails used spoofed domains for firms Boeing, Alsalam Aircraft Company, Northrop Grumman Aviation Arabia and Vinnell Arabia. Many of the victims who clicked on the link inadvertently downloaded DropShot.

APT33 group is believed to be behind a cyber-espionage campaign targeting aerospace, petrochemical and energy sector firms located in the United States, Saudi Arabia and South Korea.

Data of 46.2 million Malaysian Mobile Phone Subscribers Online

Source: https://www.reuters.com/

Malaysia is investigating an alleged attempt to sell the data of more than 46 million mobile phone subscribers online, in what appears to be one of the largest leaks of customer data in Asia. The massive data breach, believed to affect almost the entire population of Malaysia, was first reported by Lowyat.net, a local technology news website. The website said it had received a tip-off that someone was trying to sell huge databases of personal information on its forums. The country's internet regulator, the Malaysian Communications and Multimedia Commission, was looking into the matter with the police. The leaked data included lists of mobile phone numbers, identification card numbers, home addresses, and SIM card data of 46.2 million customers from at least 12 Malaysian mobile phone and mobile virtual network operators. Cybersecurity researchers said the leaked data was extensive enough to allow criminals to create fraudulent identities to make online purchases. According to a Singapore-based cybersecurity researcher, the leaked database was initially being sold on several underground forums for 1 bitcoin. At least one other user was posting a link for anyone to download it for free. The researcher, who declined to be named, said he had seen at least 10 people on an online forum in the "dark web" download the data before it was taken offline.



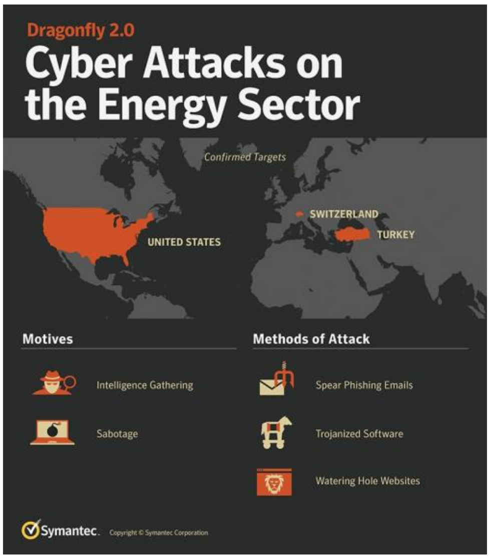
obtain all the data with the MCMC last week.

The leaked data included lists of mobile phone numbers, identification card numbers, home addresses, and SIM card data of 46.2 million customers from at least 12 Malaysian mobile phone and mobile virtual network operators.

Intruders Gaining Hands-on Access to Power Grid Operations

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

Security firm Symantec is warning that a series of recent hacker attacks not only compromised energy companies in the US and Europe but also resulted in the intruders gaining hands-on access to power grid operations—enough control that they could have induced blackouts on American soil at will. Symantec revealed a new campaign of attacks by a group Dragonfly 2.0, which it says targeted dozens of energy companies. In more than 20 cases, Symantec says the hackers successfully gained access to the target companies' networks. And at a handful of US power firms and at least one company in Turkey—none of which Symantec named—their forensic analysis found that the hackers obtained what they call operational access: control of the interfaces power company engineers use to send actual commands to equipment like circuit breakers, giving them the ability to stop the flow of electricity into US homes and businesses.



An outline of the Dragonfly group's activities in its most recent campaign. Source: www.symantec.com

Trends

Microsoft for a Cyber Equivalent of the Geneva Convention

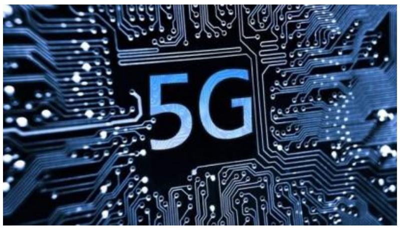
Source: http://www.theregister.co.uk

Microsoft president Brad Smith appeared before the UN in Geneva to talk about the growing problem of nation-state cyber-attacks on 9th November. During the UN session on internet governance challenges, Smith made the case for a cyber equivalent of the Geneva Convention. He started off by noting the sorry state of IoT security before arguing that tech firms and government each have a role to play in reining in the problem. "*If you can hack your way into a thermostats you can hack your way into the electric grid*," Smith said, adding that the tech sector has the first responsibility for improving internet security because "*after all we built this stuff*". International tensions are increasingly spilling out into cyberspace. "*Nation states are making a growing investment in increasingly sophisticated cyber weapons*," Smith said. "*We need a new digital Geneva Convention*." "*Government should agree not to attack civilian infrastructures, such as the electrical grid or electoral processes*," he said, adding that nation states should also agree not to steal intellectual property. Existing rules for political advertising in print and broadcast media should be extended to social media, Smith suggested. A framework to extend existing international law into the realm of cyber-conflict already exists in the shape of the Tallinn Manual. Smith argued that tech companies needed to be neutral in cyber-conflict and help their customers wherever they might be.

> *"Government should agree not to attack civilian infrastructures, such as the electrical grid or electoral processes," Smith said, adding that nation states should also agree not to steal intellectual property. - Microsoft*

5G Technology: Future Trends in Wireless Communication

Sh. Neeraj Saini, Sectoral Coordinator, Telecom, NCIIPC



Fifth Generation (5G) technology is a high speed network which promises evolutionary services in the arena of Telecom. 5G will not only be about faster speeds, but it will also address network congestion, energy efficiency, cost, and reliability to billions of people in the world and is also expected to have a transformative impact as it fuels the Internet Of Things (IoT) era. Telecom companies worldwide are embarking on early trails to realise immense potential in a lesser time to market for newer services that include IoT, virtual reality and sensor based smart transportation. 5G is the longer-term solution for when there will be potentially billions of devices connected. NCIIPC foresees trends for India's telecom sector which also requires new security aspects to be considered. With a high reliability and low latency required to control critical services and infrastructure, 5G will unlock new opportunities for public safety, governments, city managements and utility companies.

> *With a high reliability and low latency required to control critical services and infrastructure, 5G will unlock new opportunities for public safety, governments, city managements and utility companies.*

The bigger picture for 5G will witness the development of new business models. IoT applications that 5G enables are truly limitless. Once 5G is implemented the following utilities can be activated:

Broadband and Media everywhere: Users will experience broadband access in crowded areas like concerts, sporting events and festivals. 5G customers will also enjoy 4K movies downloaded in just seconds without a Wi-Fi connection.

Smart vehicles and transport: It will make roads safer and more environmentally friendly, while allowing buses and public transportation to run more efficiently. New services and business models can be supported considering sensors embedded in roads, railways and airfields to communicate to each other and/or with smart vehicles.

Critical services and infrastructure control: 5G will be a key enabler of the future digital world. For example, energy and water utilities will be capable of connecting to millions of networked devices, taking real-time, intelligent and autonomous decisions.

Critical control of remote devices: This lowers the risk of injury in hazardous environments and industries like manufacturing and mining will experience better efficiency and reduced costs.

Human and machine interaction: Users will experience smart cars that are capable of communicating with traffic lights; augmented reality and 360 degree immersive gaming and movies; and transmitting touch and texture to realise the tactile Internet.

Sensors networks: Sensors will be able to be implemented throughout farms allowing for crops to communicate moisture and fertilisation needs.

New services can be supported considering sensors embedded in roads, railways and airfields to communicate to each other and smart vehicles.

Energy and water utilities will be capable of connecting to millions of networked devices, taking real-time, intelligent and autonomous decisions.

Users will experience smart cars that are capable of communicating with traffic lights.

Sensors will be able to be implemented throughout farms allowing for crops to communicate moisture and fertilisation needs.

Stable or Unstable: Value of Bit Coin Increasing Exponentially

Sh. Aniruddha Kumar, Sectoral Coordinator, BFSI, NCIIPC

Bitcoin is a digital currency (also called crypto-currency) that is not backed by any central bank or governments. Bitcoins can be traded for goods or services with vendors who accept Bitcoins as payment. Bitcoin-to-Bitcoin transactions are made by digitally exchanging anonymous, heavily encrypted hash codes across a peer-to-peer (P2P) network. The P2P network monitors and verifies the transfer of Bitcoins between users. Each user's Bitcoins are stored in a program called a digital

wallet, which also holds each address the user sends and receives Bitcoins from, as well as a private key known only to the user. The Bitcoin network is designed to mathematically generate no more than 21 million Bitcoins and the network is set up to regulate itself to deal with inflation. Bitcoins can be spent by initiating a transfer request from a Bitcoin address in the customer's wallet to a Bitcoin address in the vendor's wallet. The initial value of 1 Bitcoin was $.003 in March 2010. Since then, the value of Bitcoin is increasing continuously. On 16 Dec 2017, it went past $19,000, having surpassed $11,000 on 29 Nov 2017 and $10,000 less than a day earlier. This has prompted many financial experts to warn of a dangerous bubble, while other commentators say that bitcoin still has a lot further to travel.

The initial value of 1 Bitcoin was $.003 in March 2010. Since then, the value of Bitcoin is increasing continuously. On 16 Dec 2017, it went past $19,000, having surpassed $11,000 on 29 Nov 2017 and $10,000 less than a day earlier.

References:

[1]https://kryptomoney.com/top-seven-reasons-why-bitcoin-price-is-increasing/

[2]http://cryptonewswire.com/?n=50&r=200&q=BTC

[3]https://www.quora.com/What-is-the-whole-concept-of-Bitcoin-Is-it-safe-to-invest-in-Bitcoins#!n=12

Vulnerability Watch

Critical Vulnerabilities in the RSA Authentication Agent

Source: https://tools.cisco.com/

Vulnerabilities in the RSA Authentication Agent for Web for Apache Web Server and RSA Authentication Agent API/SDK for C could allow an unauthenticated, remote attacker to bypass authentication restrictions and gain unauthorised access to resources on the targeted system. The vulnerability in RSA Authentication Agent for Web for Apache Web Server is due to improper input validation imposed by the affected software. An attacker could exploit this vulnerability by submitting crafted data to trigger a validation error. This vulnerability is only exploitable when the RSA Authentication Agent for Web for Apache Web Server has TCP protocol configured for communication with the RSA Authentication Manager server. Vulnerability in RSA Authentication Agent API/SDK for C is due to improper handling of API/SDK return codes by the affected software. An attacker could exploit this vulnerability by triggering an error handling flaw in the affected software. This vulnerability does not affect RSA Authentication Agent API/SDK for Java.

Vulnerabilities in the RSA Authentication Agent for Web for Apache Web Server and RSA Authentication Agent API/SDK for C could allow an unauthenticated, remote attacker to bypass authentication restrictions.

Critical Vulnerability in the tinysvcmdns Library

Source: https://tools.cisco.com/

Vulnerability in the tinysvcmdns library could allow an unauthenticated, remote attacker to execute arbitrary code. The vulnerability is due to improper processing of crafted DNS packets by an application using the affected library. An attacker could exploit this vulnerability by sending crafted DNS packets to a targeted system.

An attacker could exploit this vulnerability by sending crafted DNS packets to a targeted system.

Critical Vulnerability in the REST API of Cisco IOS XE Software

Source: https://tools.cisco.com/

Vulnerability in the REST API of the web-based user interface (web UI) of Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass authentication to the REST API of the web UI of the affected software. The vulnerability is due to insufficient input validation for the REST API of the affected software. An attacker could exploit this vulnerability by sending a malicious API request to an affected device. This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS XE Software, if the HTTP Server feature is enabled for the device. The newly redesigned, web-based administration UI was introduced in the Denali 16.2 Release of Cisco IOS XE Software. This vulnerability does not affect the web-based administration UI in earlier releases of Cisco IOS XE Software.

This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS XE Software, if the HTTP Server feature is enabled for the device.

Critical Vulnerability Affecting Oracle Identity Manager

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

Oracle released a security alert regarding critical vulnerability (CVE-2017-10151) affecting Oracle Identity Manager. This vulnerability has a CVSS v3 base score of 10.0, and can result in complete compromise of Oracle Identity Manager via an unauthenticated network attack. The users of enterprise identity management system are urged to apply emergency update to stop a bug that allows attackers take over the system. Oracle described the flaw as "easily exploitable". It allows "unauthenticated attacker with network access via HTTP to compromise Oracle Identity Manager".

This vulnerability has a CVSS v3 base score of 10.0, and can result in complete compromise of Oracle Identity Manager via an unauthenticated network attack.

Multiple Vulnerabilities in Oracle Tuxedo

Source: https://arstechnica.com/

Oracle issued a set of urgent security fixes that repair vulnerabilities revealed by researchers from the managed security provider ERPScan at the DeepSec security conference in Vienna, Austria.

The five vulnerabilities include one dubbed "JoltandBleed" by the researchers because of its similarity to the HeartBleed vulnerability. JoltandBleed is a serious vulnerability that could expose entire business applications running on PeopleSoft platforms accessible from the public Internet. According to recent research by ERPScan, more than 1,000 enterprises have their PeopleSoft systems exposed to the Internet. JoltandBleed is memory leakage vulnerability in Oracle's proprietary Jolt protocol, used by the Tuxedo 2 application server. Crafted network packets sent to the HTTP port controlled by the Jolt service could potentially extract data from memory on the app server, including session information, user names, and passwords in plain text. The other vulnerabilities disclosed include other memory-based attacks, including heap and stack overflow attacks, as well as a brute-force attack against passwords.

JoltandBleed is a serious vulnerability that could expose entire business applications running on PeopleSoft platforms accessible from the public Internet.

Critical Vulnerability in iniNet SCADA Webserver

Source: https://ics-cert.us-cert.gov/advisories/ICSA-17-264-04

Improper Authentication vulnerability has been identified in iniNet Solutions GmbH's SCADA Webserver. Successful exploitation of this vulnerability could allow malicious users to access human-machine interface (HMI) pages or to modify programmable logic controller (PLC) variables without authentication. IniNet Solutions GmbH has released a new version of the SCADA Webserver, V2.02.0100, which allows users to implement basic authentication. CVE-2017-13995 has been assigned to this vulnerability. A CVSS v3 base score of 10.0 has been assigned.

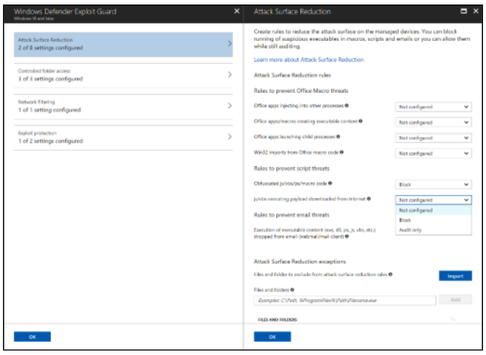
Successful exploitation of this vulnerability could allow to access human-machine interface pages or to modify programmable logic controller variables.

Security App

Windows Defender Exploit Guard

Source: https://blogs.technet.microsoft.com/

Windows Defender Exploit Guard is a new set of intrusion prevention capabilities that ships with the Windows 10 Fall Creators Update. The four components of Windows Defender Exploit Guard are designed to lock down the device against a wide variety of attack vectors and block behaviours commonly used in malware attacks. Despite advances in antivirus detection capabilities, attackers are continuously adapting and have been expanding their arsenal of tricks and techniques to compromise endpoints, steal credentials, and execute ransomware attacks without ever needing to write anything to disk. Windows Defender Exploit Guard utilizes the capabilities of the Microsoft Intelligent Security Graph (ISG) and the security research team at Microsoft to identify active



Windows Defender Exploit Guard
Windows 10 and later

Attack Surface Reduction
2 of 8 settings configured

Controlled folder access
3 of 3 settings configured

Network filtering
1 of 1 setting configured

Exploit protection
1 of 2 settings configured

Attack Surface Reduction

Create rules to reduce the attack surface on the managed devices. You can block running of suspicious executables in macros, scripts and emails or you can allow them while still auditing.

Learn more about Attack Surface Reduction

Attack Surface Reduction rules

Rules to prevent Office Macro threats

Office apps injecting into other processes: Not configured

Office apps/macros creating executable content: Not configured

Office apps launching child processes: Not configured

Win32 imports from Office macro code: Not configured

Rules to prevent script threats

Obfuscated js/vbs/ps/macro code: Block

js/vbs executing payload downloaded from Internet: Not configured

Rules to prevent email threats

Execution of executable content (exe, dll, ps, js, vbs, etc.) dropped from email (webmail/mail client)

Attack Surface Reduction exceptions

Files and folder to exclude from attack surface reduction rules

Files and folders

Examples: C:\Path, %ProgramFiles%\Path\Filename.exe

FILES AND FOLDERS

Four Components are designed to lock down the device against a wide variety of attack vectors.

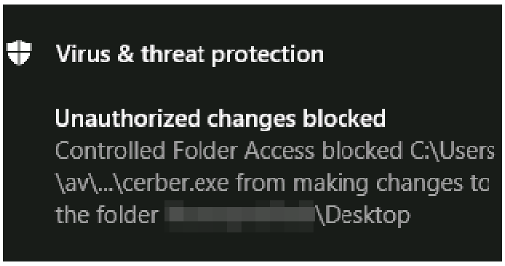
exploits and common behaviours to stop these types of attacks at various stages of the kill chain. By correlating streams of events to various malicious behaviours with the ISG, Windows Defender Exploit Guard provides the capability and controls needed to handle these types of emerging threats. The four components of Windows Defender Exploit Guard are:

Attack Surface Reduction (ASR): A set of controls that enterprises can enable to prevent malware from getting on the machine by blocking Office-, script-, and email-based threats

Network protection: Protects the endpoint against web-based threats by blocking any outbound process on the device to untrusted hosts/IP through Windows Defender SmartScreen

Controlled folder access: Protects sensitive data from ransomware by blocking untrusted processes from accessing your protected folders

Exploit protection: A set of exploit mitigations (replacing EMET) that can be easily configured to protect system and applications


Virus & threat protection

Unauthorized changes blocked
Controlled Folder Access blocked C:\Users\av\...\cerber.exe from making changes to the folder [redacted]\Desktop

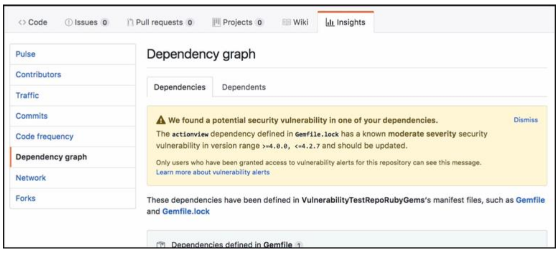
Controlled folder access blocks unauthorized access and notifies the user of any attempt by unauthorized apps to access or modify files in protected folders. It delivers this protection in real-time.

Protects the endpoint against web-based threats by blocking any outbound process to untrusted hosts/IP.

GitHub Vulnerability Detection Service

Source: http://www.zdnet.com

Development platform GitHub has launched a new service that searches project dependencies in JavaScript and Ruby for known vulnerabilities and then alerts project owners if it finds any. The new service aims to help developers update project dependencies as soon as GitHub becomes aware of a newly announced vulnerability. GitHub will identify all public repositories that use the affected version of the dependency. Projects under private repositories will need to opt into the vulnerability-detection service. The alerts form part of GitHub's so-called 'dependency graph', which helps developers monitor projects that their code depends on. Developers can view the security alerts in the repository's dependency graph, which can be accessed from 'Insights'. The alerts are only sent to project owners and others with admin access to repositories. The company promises never to publicly disclose vulnerabilities for a specific repository. Users can choose to receive the alerts by email, web notifications or the GitHub interface. GitHub's is also using machine learning to suggest fixes from the GitHub community.



Dependency graph

We found a potential security vulnerability in one of your dependencies.
The `actionview` dependency defined in `Gemfile.lock` has a known **moderate severity** security vulnerability in version range `>=4.0.0, <=4.2.7` and should be updated.

Only users who have been granted access to vulnerability alerts for this repository can see this message.
Learn more about vulnerability alerts

These dependencies have been defined in **VulnerabilityTestRepoRubyGems**'s manifest files, such as Gemfile and Gemfile.lock

Dependencies defined in Gemfile 1

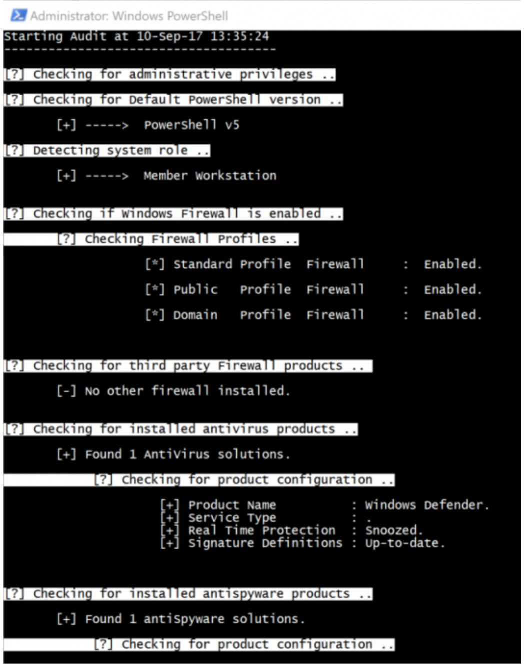
Developers can view the security alerts in the repository's dependency graph, which can be accessed from 'Insights'. Image: GitHub

The new service aims to help developers update project dependencies as soon as GitHub becomes aware of a newly announced vulnerability.

WINSpect - Windows Security Auditing Toolbox

Source: https://isc.sans.edu/

WINSpect is a Powershell based Windows Security Auditing Toolbox.



```
Starting Audit at 10-Sep-17 13:35:24
----------------------------------------

[?] Checking for administrative privileges ..

[?] Checking for Default PowerShell version ..

       [+] ----->  PowerShell v5

[?] Detecting system role ..

       [+] ----->  Member Workstation


[?] Checking if Windows Firewall is enabled ..

       [?] Checking Firewall Profiles ..

                   [*] Standard Profile  Firewall     :  Enabled.

                   [*] Public   Profile  Firewall     :  Enabled.

                   [*] Domain   Profile  Firewall     :  Enabled.



[?] Checking for third party Firewall products ..

       [-] No other firewall installed.

[?] Checking for installed antivirus products ..

       [+] Found 1 AntiVirus solutions.

            [?] Checking for product configuration ..

                     [+] Product Name           : Windows Defender.
                     [+] Service Type           : .
                     [+] Real Time Protection   : Snoozed.
                     [+] Signature Definitions  : Up-to-date.


[?] Checking for installed antispyware products ..

       [+] Found 1 antiSpyware solutions.

            [?] Checking for product configuration ..
```

It focuses on enumerating different parts of a Windows machine to identify security weaknesses and point to components that need further hardening.

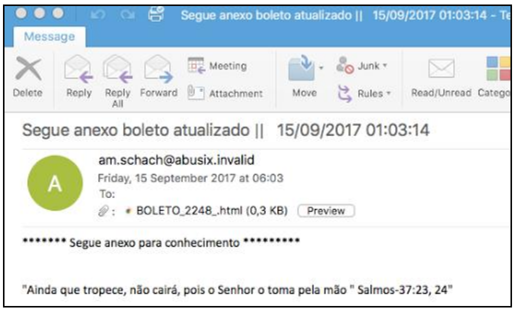
WINspect is part of a larger project for auditing different areas of Windows environments. It focuses on enumerating different parts of a Windows machine to identify security weaknesses and point to components that need further hardening. This current version of the script supports the following features:

- Checking for installed security products.
- Checking for DLL hijackability (Authenticated Users security context).
- Checking for User Account Control settings.
- Checking for unattended installs leftovers.
- Enumerating world-exposed local filesystem shares.
- Enumerating domain users and groups with local group membership.
- Enumerating registry autoruns.
- Enumerating local services that are configurable by Authenticated Users group members.
- Enumerating local services for which corresponding binary is writable by Authenticated Users group members.
- Enumerating non-system32 Windows Hosted Services and their associated DLLs.
- Enumerating local services with unquoted path vulnerability.
- Enumerating non-system scheduled tasks.

Malware Bytes

Malware Targeting the Brazilian Financial Sector

Source: https://www.scmagazine.com/



Segue anexo boleto atualizado || 15/09/2017 01:03:14 - Te

Segue anexo boleto atualizado || 15/09/2017 01:03:14

am.schach@abusix.invalid
Friday, 15 September 2017 at 06:03
To:
: BOLETO_2248_.html (0,3 KB)

******* Segue anexo para conhecimento *********

"Ainda que tropece, não cairá, pois o Senhor o toma pela mão " Salmos-37:23, 24"

Attackers send victims spam messages written in Portuguese enticing them to open a Boleto invoice Image: https://blog.talosintelligence.com/2017/09/brazilbanking.html

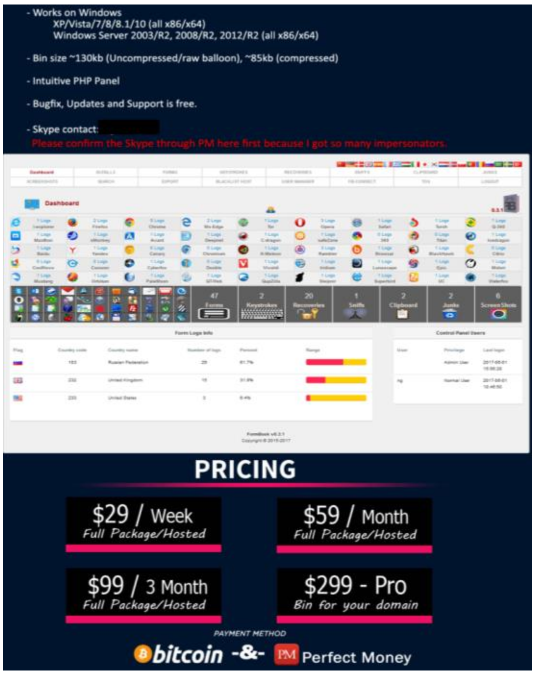
The Trojan uses an authentic VMware binary to deceive security tools into accepting errant activity and to bypass security checks.

Cybercriminals are using legitimate VMware binary to spread banking Trojans in a new phishing campaign targeting the Brazilian financial sector. Attackers send victims spam messages written in Portuguese enticing them to open a Boleto invoice, a popular Brazilian payment method. The phishing emails contains a file with a URL that redirects users to a goo.gl URL shortener, then sends them to a RAR library that contains a JAR file. If a victim double-clicks the JAR file, it triggers a Java process that initializes malicious code and installs the banking Trojan. The Trojan uses an authentic VMware binary to deceive security tools into accepting errant activity and to bypass security checks because if the initial binary, such as vm.png, is accepted, then the security tools assume that subsequent libraries will also be trustworthy. The malware is also packed with the Themida commercial packet which makes it difficult to analyse. Trojan uses a wide range of techniques to stay hidden with the goal of stealing banking credentials from the user.

FormBook Malware Targeting Firms in US and South Korea

Source: https://threatpost.com/

Attackers spreading new malware called FormBook are singling out aerospace firms, defence contractors and some manufacturing organisations in the United States and South Korea. According to researchers at FireEye, FormBook was spotted in several high-volume distribution campaigns targeting the US with email containing malicious PDF, DOC or XLS attachments. FormBook targets in South Korea are being pelted with email containing malicious archive files (ZIP, RAR, ACE, and ISOs) with executable payloads. FormBook is a type of data-stealing malware used in espionage and is capable of keystroke logging, stealing clipboard contents and extracting data from HTTP sessions. Once installed, the malware can also execute commands from a command-and-control (C2) server such as instructing the malware to download more files, start processes, shutdown and reboot a system and steal cookies and local passwords. FormBook has been sold in underground hacking forums since July for US$29 a week to a US$299 full-package "pro" deal. FireEye detected two distinct email campaigns between August 11 and 22 and an additional campaign between July 18 and August 2017. In a PDF campaign hackers leveraged FedEx and DHL shipping and package delivery themes. PDFs contained links to the "tny.im" URL-shortening service, which then redirected to a staging server that contained FormBook executable payloads.



- Works on Windows
  XP/Vista/7/8/8.1/10 (all x86/x64)
  Windows Server 2003/R2, 2008/R2, 2012/R2 (all x86/x64)

- Bin size ~130kb (Uncompressed/raw balloon), ~85kb (compressed)

- Intuitive PHP Panel

- Bugfix, Updates and Support is free.

- Skype contact: [redacted]
Please confirm the Skype through PM here first because I got so many impersonators.

PRICING

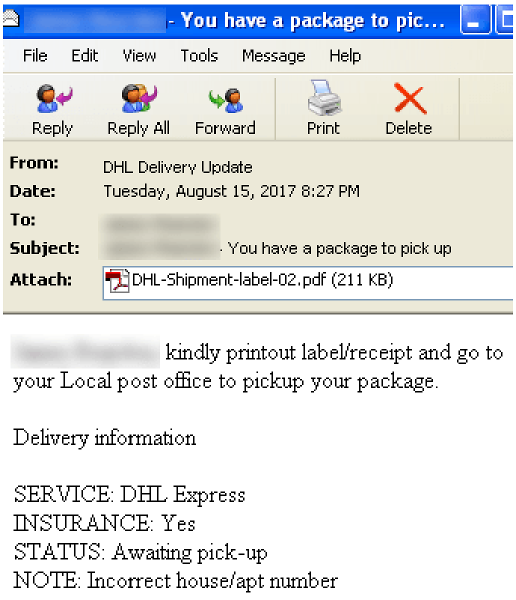
$29 / Week
Full Package/Hosted

$59 / Month
Full Package/Hosted

$99 / 3 Month
Full Package/Hosted

$299 - Pro
Bin for your domain

PAYMENT METHOD
bitcoin -&- PM Perfect Money



From: DHL Delivery Update
Date: Tuesday, August 15, 2017 8:27 PM
To: [redacted]
Subject: [redacted] - You have a package to pick up
Attach: DHL-Shipment-label-02.pdf (211 KB)

[redacted] kindly printout label/receipt and go to your Local post office to pickup your package.

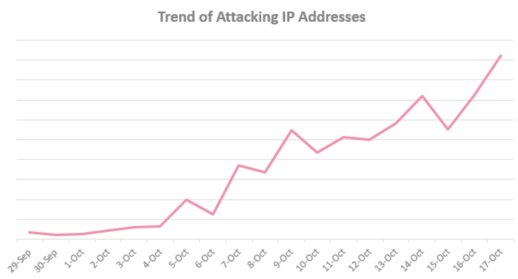
Delivery information

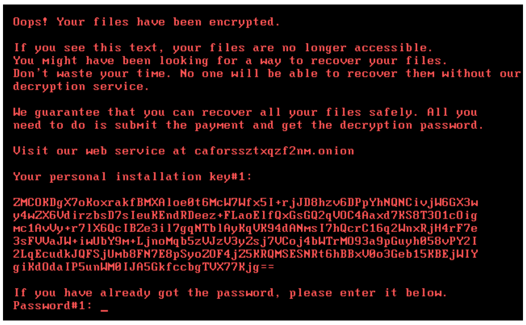
SERVICE: DHL Express
INSURANCE: Yes
STATUS: Awaiting pick-up
NOTE: Incorrect house/apt number

Botnet, Dubbed 'IoTroop', Evolving and Recruiting IoT Devices

Source: https://research.checkpoint.com/new-iot-botnet-storm-coming/

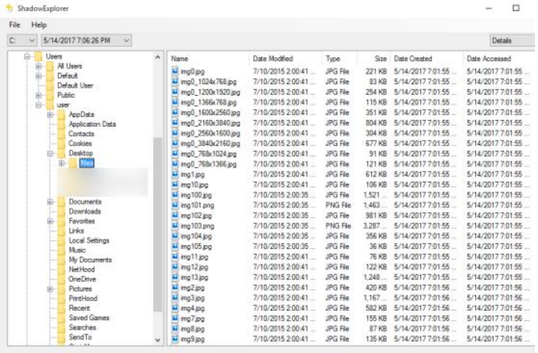
Check Point Researchers have discovered a brand new Botnet, dubbed 'IoTroop', evolving and recruiting IoT devices at a far greater pace and with more potential damage than the Mirai botnet of 2016. Ominous signs were first picked up via Check Point's Intrusion Prevention System (IPS) in the last few days of September. An increasing number of attempts were being made by hackers to exploit a combination of vulnerabilities found in various IoT devices. With each passing day the malware was evolving to exploit an increasing number of vulnerabilities in Wireless IP Camera devices such as GoAhead, D-Link, TP-Link, AVTECH, NETGEAR, MikroTik, Linksys, Synology and others. It soon became apparent that the attempted attacks were coming from many different sources and a variety of IoT devices, meaning the attack was being spread by the IoT devices themselves. It is early to assess the intentions of the threat actors behind it, but it is vital to have the proper preparations and defence mechanisms in place before an attack strikes.





```
Oops! Your files have been encrypted.

If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.

We guarantee that you can recover all your files safely. All you
need to do is submit the payment and get the decryption password.

Visit our web service at caforssztxqzf2nm.onion

Your personal installation key#1:

ZMCOKDgX7oKoxrakfBMXAloe0t6McW7Wfx5I+rjJD8hzv6DPpYhNQNCivjW6GX3w
y4wZX6VdirzbsD7sIeuKEndRDeez+FLaoElfQxGsGQ2qVOC4Aaxd7KS8T3O1cOig
mc1AvVy+r7lX6QcIBZe3il7gqNTblAyKqVK94dANmsI7hQcrC16q2WnxRjH4rF7e
3sFVVaJW+iwUbY9m+LjnoMqb5zVJzV3yZsj7VCoj4bWTrMO93a9pGuyh058vPY2I
2LqEcudkJQFSjUmb8FN7E8pSyoZOF4jZ5KRQMSESNRt6hBBxV0o3Geb15KBEjWIY
giKdOdaIP5unWM0IJA5GkfccbgTVX77Kjg==

If you have already got the password, please enter it below.
Password#1: _
```

Here's what a ransom message looks like for the unlucky victims



Name	Date Modified	Type	Size	Date Created	Date Accessed
img0.jpg	7/10/2015 2:00:41 ...	JPG File	221 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img0_1024x768.jpg	7/10/2015 2:00:41 ...	JPG File	83 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img0_1200x1920.jpg	7/10/2015 2:00:41 ...	JPG File	254 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img0_1366x768.jpg	7/10/2015 2:00:41 ...	JPG File	115 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img0_1600x2560.jpg	7/10/2015 2:00:41 ...	JPG File	351 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img0_2160x3840.jpg	7/10/2015 2:00:41 ...	JPG File	804 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img0_2560x1600.jpg	7/10/2015 2:00:41 ...	JPG File	304 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img0_3840x2160.jpg	7/10/2015 2:00:41 ...	JPG File	677 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img0_768x1024.jpg	7/10/2015 2:00:41 ...	JPG File	91 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img0_768x1366.jpg	7/10/2015 2:00:41 ...	JPG File	121 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img1.jpg	7/10/2015 2:00:41 ...	JPG File	612 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img10.jpg	7/10/2015 2:00:41 ...	JPG File	106 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img100.jpg	7/10/2015 2:00:35 ...	JPG File	1,521 ...	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img101.png	7/10/2015 2:00:35 ...	PNG File	1,463 ...	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img102.jpg	7/10/2015 2:00:35 ...	JPG File	981 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img103.png	7/10/2015 2:00:35 ...	PNG File	3,287 ...	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img104.jpg	7/10/2015 2:00:35 ...	JPG File	356 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img105.jpg	7/10/2015 2:00:35 ...	JPG File	36 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img11.jpg	7/10/2015 2:00:41 ...	JPG File	76 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img12.jpg	7/10/2015 2:00:41 ...	JPG File	122 KB	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img13.jpg	7/10/2015 2:00:41 ...	JPG File	1,248 ...	5/14/2017 7:01:55 ...	5/14/2017 7:01:55 ...
img2.jpg	7/10/2015 2:00:41 ...	JPG File	420 KB	5/14/2017 7:01:56 ...	5/14/2017 7:01:56 ...
img3.jpg	7/10/2015 2:00:41 ...	JPG File	1,167 ...	5/14/2017 7:01:56 ...	5/14/2017 7:01:56 ...
img4.jpg	7/10/2015 2:00:41 ...	JPG File	582 KB	5/14/2017 7:01:56 ...	5/14/2017 7:01:56 ...
img7.jpg	7/10/2015 2:00:41 ...	JPG File	155 KB	5/14/2017 7:01:56 ...	5/14/2017 7:01:56 ...
img8.jpg	7/10/2015 2:00:41 ...	JPG File	87 KB	5/14/2017 7:01:56 ...	5/14/2017 7:01:56 ...
img9.jpg	7/10/2015 2:00:41 ...	JPG File	135 KB	5/14/2017 7:01:56 ...	5/14/2017 7:01:56 ...

Shadow copies remain unharmed by Bad Rabbit

Mass Attacks with Ransomware called Bad Rabbit

Source: https://securelist.com/bad-rabbit-ransomware/82851/

On October 24th we observed notifications of mass attacks with ransomware called Bad Rabbit. It targeted organisations and consumers, mostly in Russia but there were reports of victims in Ukraine, Turkey and Germany. The ransomware dropper was distributed with the help of drive-by attacks. While the target is visiting a legitimate website, a malware dropper is being downloaded from the threat actor's infrastructure. No exploits were used, so the victim would have to manually execute the malware dropper, which pretends to be an Adobe Flash installer. However, analysis confirmed that Bad Rabbit uses the EternalRomance exploit as an infection vector to spread within corporate networks. The same exploit was used in the ExPetr. A number of compromised websites, of news or media were detected. Overall, there were almost 200 targets, according to the KSN statistics. The server from which the Bad rabbit dropper was distributed went down. Bad Rabbit ransomware encrypts a victim's files and disk. Files are encrypted with AES-128-CBC and RSA-2048 algorithms. It is a default encryption scheme for ransomware. Bad Rabbit does not delete shadow copies after encrypting the victim's files. It means that if the shadow copies had been enabled prior to infection and if the full disk encryption did not occur for some reason, then the victim can restore the original versions of the encrypted files by the means of the standard Windows mechanism or 3rd-party utilities.

Black Swan Ransomware Attack

Sh. Aniruddha Kumar, Sectoral Coordinator, BFSI, NCIIPC

In a Black swan ransomware attack, the perpetrator compromises business of a company, as well as business backup hosted on cloud services such as Amazon or Microsoft Azure, resulting in the company being locked out of both data and data backups. It is a dual ransomware attack on both data as well as data backups. A good Disaster Recovery (DR) plan and Data backup up do not mean one can defeat a ransomware attack. The company's ability to secure its data, along with its own infrastructure is critical to survival. Three years ago, Code Spaces faced a black swan event and within days, the company shut down its operations. While highly prepared for a conventional DR event, the company's fatal mistake was that its business and sensitive company data was hosted in the same cloud (Amazon Web Service's) and accessible via the same credentials. The company experienced a DDoS attack, which occurs when multiple systems flood the bandwidth of the company's servers. Unknown to Code Spaces, the perpetrators had hacked into their AWS EC2 management console.

It is a dual ransomware attack on both data as well as data backups.

When a ransom was denied, the perpetrators deleted the entirety of the company's files, including both its production data and backup copy, and the company was finished.

Mitigation Methodology

Create air gap: Maintain periodic "air gap" copies of data on tape or other offline media and store it offsite where it is inaccessible via network. Do not host business and business data on same cloud/server.

> *Maintain periodic "air gap" copies of data on tape or other offline media and store it offsite where it is inaccessible via network.*

Test the backups: We should periodically restore and test a sample of backups to assure their integrity. Verify a periodic sample of backups to avoid a potentially nasty surprise if we lose data to a ransomware attack and then find our backups are defective.

References:

[1]http://searchitchannel.techtarget.com/tip/Black-swan-event-Preparing-for-a-dual-ransomware-attack

[2]https://www.financierworldwide.com/preparing-for-a-black-swan-cyber-event/#.WiUoPzThUdU

Learning

OWASP Top 10 – 2017, Top Web Application Security Risks

Source: https://www.owasp.org/

A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risks problem areas, and provides guidance on where to go from here.

> *The Top 10 provides basic techniques to protect against these high risks problem areas, and provides guidance on where to go from here.*

A1:2017-Injection: Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorisation.

A2:2017-Broken Authentication: Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

A3:2017-Sensitive Data Exposure: Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser

A4:2017-XML External Entities (XXE): Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks

A5:2017-Broken Access Control: Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorised functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

A6:2017-Security Misconfiguration: Security misconfiguration is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.

A7:2017-Cross-Site Scripting (XSS): XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8:2017-Insecure Deserialization: Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

A9:2017-Using Components with Known Vulnerabilities: Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defences and enable various attacks and impacts.

A10:2017-Insufficient Logging & Monitoring: Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

A1:2017-Injection

A2:2017-Broken Authentication

A3:2017-Sensitive Data Exposure

A4:2017-XML External Entities

A5:2017-Broken Access Control

A6:2017-Security Misconfiguration

A7:2017-Cross-Site Scripting

A8:2017-Insecure Deserialization

A9:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging & Monitoring

To Make Internet of Things More Secure

Source: https://www.us-cert.gov/ncas/tips/ST17-001

The Internet of Things (IoT) refers to any object or device that sends and receives data automatically through the Internet. This technology provides a level of convenience to our lives, but it requires that we share more information than ever. The security of this information, and the security of these devices, is not always guaranteed. Attackers take advantage of this scale to infect large segments of devices at a time, allowing them access to the data on those devices or to, as part of a botnet, attack other computers or devices for malicious intent. Without a doubt, the IoT makes our lives easier and has many benefits; but we can only reap these benefits if our Internet-enabled devices are secure and trusted. The following are important steps should be considered to make them more secure.

Drawing that represents the Internet of Things. Includes connected objects, a drone, a connected plant. Source: Wikipedia.org

Evaluate security settings: It is important to examine the settings, particularly security settings, and select options that meet needs without putting at increased risk. If a patch or a new version of software is installed, or if there is something that might affect device, re-evaluate the settings to make sure they are still appropriate.

Ensure up-to-date software: Patches are software updates that fix a particular issue or vulnerability within device's software. Make sure to apply relevant patches as soon as possible.

Connect carefully: Once device is connected to the Internet, it's also connected to millions of other computers, which could allow attackers access to device. Consider whether continuous connectivity to the Internet is needed.

Use strong passwords: Some Internet-enabled devices are configured with default passwords to simplify setup. These default passwords are easily found online, so they don't provide any protection. Choose strong passwords to secure device.

Examine the settings, and select options that meet needs without putting at increased risk.

Apply relevant patches as soon as possible.

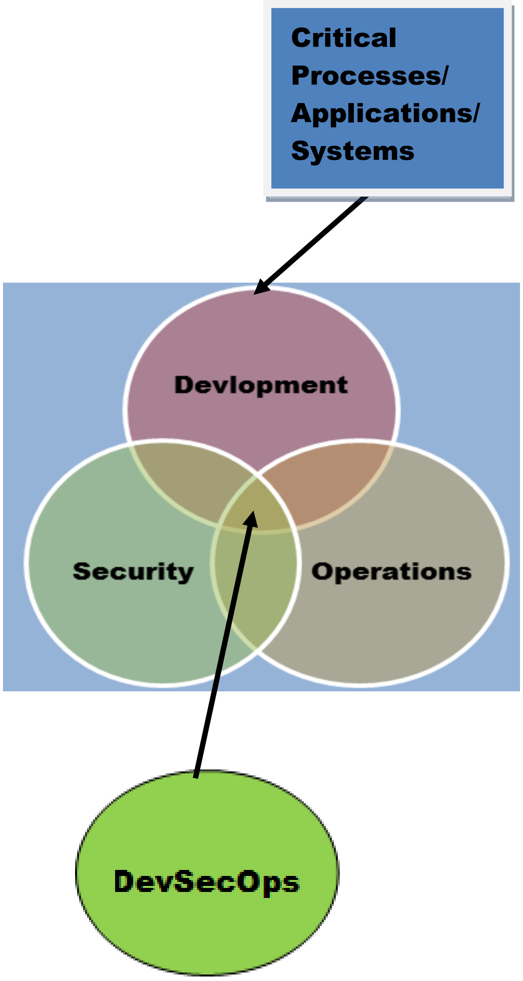
Consider whether continuous connectivity to the Internet is needed.

Choose strong passwords.

Security is Everyone's Responsibility: DevSecOps

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

DevOps (Development + Operations) under Software Engineering is one of the best practices for amalgamation of Software and Development operations through regular automation and monitoring. DevOps strikes a balance between the business needs and speed of delivery due to numerous iteration processes which arises due to reasons viz. customer requirements, technological evolution, consumer feedbacks, ambit expansions etc. With DevOps, IT companies now have the capability for building custom system quickly, with greater flexibility and lower cost. But these frequent



iterations creates inherent risks and challenges which in traditional security operations are missed, as all the security defences are embedded after the system is designed. All the security challenges and issues as raised in the DevOps tends to be addressed by DevSecOps where the aim is to make security and compliance available to be consumed as services by integrating security at multiple levels into DevOps workflows, which helps in identifying the security issues in the development process rather than post release. As highlighted in the figure, DevSecOps is everyone's responsibility with coherently and effectively embedding the security controls including synchronisation with the scale and speed of Development and operations. Usually in cloud based deployment DevSecOps address the security processes at three layers viz. Infrastructure, Platform and Application.

All the security challenges and issues as raised in the DevOps tends to be addressed by DevSecOps where the aim is to make security and compliance available to be consumed as services by integrating security at multiple levels into DevOps workflows, which helps in identifying the security issues in the development process rather than post release.

Best practices for adopting DevSecOps: Indicative checklist

- Secure coding, involving best practices embedded during the code development phase starting at the design level.
- Baseline hardening and Configuration management, taking care of pre-shipped default configurations, information disclosures and errors arising out of frequent iterations.
- Immutable systems, which cannot be tempered once deployed and implemented properly.
- Phoenix upgrades, only allows immaculate upgrades keeping it as the known good in the repository discarding the other ones.
- Exhaustive and automated auditing taking into account all the logs of access controls, changes, administrative accesses, remote access etc.
- Automated security processes should be part of the continuous development process e.g. system hardening, upgrades, updates and testing. Continuous and rigorous testing will identify the gap areas arising out of iterations.
- Data protection should inherently be part of the continuous integration process to keep abreast of the latest trends while infusing the necessary amendments at the development stage itself.
- Security Operation Centre, should keep tab of the access attempts, events types, date and time stamp, success or failures, origination, changes made etc.
- All the communications with use of “restful” application programme interface between multiple systems for integration purposes including third party accesses should be thoroughly validated, authorised and hardened.

Real time communication and collaboration in the DevSecOps environment with the inclusion of board members is must to make cyber security everybody's responsibility.

Artificial Intelligence for Cyber Security in ICS/SCADA Systems

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

Artificial Intelligence (AI) is problem solving or learning activities performed by machines. A good example of AI usage is self-driving cars. AI can be of great help in cyber security domain, especially for Industrial Control Systems (ICS) and Supervisory Data Acquisition & Control (SCADA) systems, as these systems generate huge volume of event/alert data for Security Operation Centres. A general Security Events and Incident Management (SIEM) solution may not be able to apply intelligence and detect the threat. Further, it may not be feasible for the Incident Response Team to manually analyse all the alerts. In such scenario, an AI based solution may assist significantly, as it can mimic cognitive functionality of human minds and analyse the volume data. Further, it may assist to take suitable prevention course of actions. An example may be, detection and categorisation of a code reaching to SCADA LAN through opening of some phishing email attachment at the DMZ (De-Militarised Zone) by correlating logs of DMZ and MZ devices; issuing alert to multiple Anti malware solutions to cross verify segregating the compromised zone and applying a Access Control Filter at Firewalls to prevent in-flow traffic to the Command-and-Control Centre; generating a token for Incident Response Team for Forensics, etc. There are several AI based ICS/SCADA security products available which provides continuous Risk Assessment, threat/anomaly detection and prevention logics, however while implementing the product, a CII organisation needs to take into the account various security and business parameters, these include:

An AI based solution may assist significantly, as it can mimic cognitive functionality of human minds and analyse the volume data.

- Multi-vendor ICS/SCADA product support
- Having non-invasive functionalities
- Not affecting operational resiliency of the CII assets
- Supporting open-source architecture and scalabilities (multi-site support)
- Providing fast-track patches and support for the vulnerabilities detected within the product itself
- Avoid data/telemetry exfiltration to cloud

Monitoring Encrypted Traffic: Strategies

Sh. Shiv Charan Kataria, NCIIPC

Encryption while enforced to implement security in Internet traffic, has in practice made security monitoring by perimeter devices difficult. Generally organisations choose to pass encrypted traffic into their networks without screening. This creates "Blind Spots" in networks. These blind spots are being exploited by attackers. Ponemon Institute reported that 40 percent of cyber-attacks leverage Secure Socket Layer. Earlier the encryption was used only for sensitive traffic, now encryption being cheaper is becoming a norm and the Internet is approaching towards almost 100 percent encryption. The best way to monitor the encrypted traffic is to first decrypt and passing it to security devices, but this is time consuming even when the cryptographic key is available which is not in most of the time. The projected migration from 1024 to 2048 bit cypher will further complicate the case. What then is the strategy to face the challenge in a cost effective way? The following strategies summarise the best available solutions.

Purging Malicious Traffic: Using the Threat Intelligence Gateways (TIG) and Cyber Advanced Warning Systems (CAWS) detection of malicious traffic is possible using the IP address of the packet header; which is in clear text. TIG and CAWS compare the IP address with a large continuously updated malicious database of IP addresses. The crux of this approach is to maintain an up to mark threat database. Based on the industry, the TIG can achieve up to 80 percent reduction in encrypted traffic.

Cost-Effective Scalable Architecture: After purging malicious traffic from suspicious IP address the remaining traffic can be decrypted as it is smaller in volume. Some of the latest Firewalls, Intrusion Detection Systems and Unified Threat Intelligence Systems offer an additional feature of SSL decryption. Decryption but is a process-intensive function that slows the performance of deep packet inspection tools and can potentially create serious bottlenecks. This would require sooner than projected capacity upgradation. Centralised decryption then provides a cost effective solution by minimising CPU cycles devoted to decryption and lets the information be quickly delivered to multiple tools at the same time. Network Packet Brokers increase tool efficiency by sorting through all the network traffic by identifying relevant packets for each tool, and distributing the traffic to tools at high speed.

Futuristic Procurements: As encryption becomes the norm, the attack frequency will tend to rise. The quality of decryption tools will become more important in achieving total network visibility. Hence the security solution must support the latest and upcoming standards and must cater wide variety of ciphers and algorithms. The capacity to handle wide variety of SSL traffic will give resilience to denial of service attacks.

Fighting Interception: With centralised decryption data moves to various security devices in plaintext. This plaintext data is vulnerable to interception. It increases the overall "attack surface".

Ponemon Institute reported that 40 percent of cyber-attacks leverage Secure Socket Layer.

After purging malicious traffic from suspicious IP address the remaining traffic can be decrypted as it is smaller in volume.

The security solution must support the latest and upcoming standards and must cater wide variety of ciphers and algorithms.

That means login information, financial transactions, social security numbers, healthcare data, phone numbers, and anything else that was encrypted for security purpose is now readable by anyone that can intercept the traffic or access the tools that receive it. To mitigate the risk of interception we must use additional security measures on packets before they reach tools. Another way is to trim off any part of the packet that is not necessary to the inspection process before it is sent to security tools.

To mitigate the risk of interception we must use additional security measures on packets before they reach tools.

With growing ICT and encryption the attack surface is tend to grow, thus it is essential to inspect all encrypted network traffic.

References:

[1]https://www.ixiacom.com/sites/default/files/2017-05/915-8155-01-5071%20WP%20Best%20Practices%20for%20Monitoring%20Encrypted%20Data.pdf

Preparation of Cyber Crisis Management Plan

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

Cyber security incident is a crisis scenario that every organisation is vulnerable to, which makes it one of the high-risk scenarios to include within crisis preparedness program. Cyber Crisis Management Plan (CCMP) is the document which helps organisation in handling such scenarios. Organisation while formulating CCMP may include following section during preparation of CCMP for Critical Information Infrastructure (CII).

- While preparing CCMP in an organisation, consideration of CII component should be viewed in holistically with third party organisation, inter / intra organisational dependencies and functional dependencies.
- For operational requirements organisation require sharing CCMP document with third party organisation / System Integrator / Vendors etc., hence proper classification of the document is required. Detailed information like IP, network equipment details should be avoided for CII components and as far as possible defined in broader terms.
- A section in the document should clearly mention that the sharing of cyber incidence report with NCIIPC for CII/Protected Systems is mandatory. For incident scope spanning in multiple states and national level, notify the incidents to NCIIPC to avert any critical services to be hit during the incident.
- It is suggested to include NCIIPC control guidelines ver2.0 as reference document applicable for CII systems in CCMP.

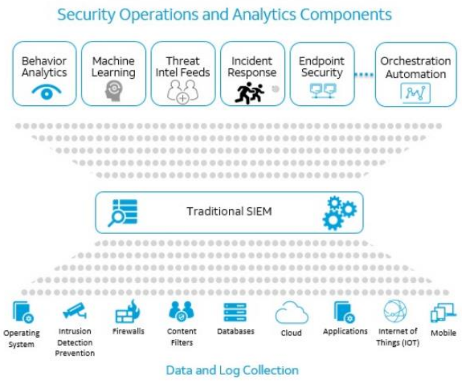
A section in the document should clearly mention that the sharing of cyber incidence report with NCIIPC for CII/Protected Systems is mandatory.

- Incorporate NCIIPC contact details in CCMP document for ready reference.
- CCMP mock drill plan for CII components should be defined separately and with minimum timeframe as per the organisational Information security policy.

CII organisations can forward the CCMP documents to NCIIPC for review and consultation. This will help in close coordination of NCIIPC and CII organisation in protecting critical national assets.

Security Operations and Analytics Platform Architecture

Sh. Niraj Vishnoi, NCIIPC



Security Operations and Analytics Platform Architecture Overview

A leading market research company has published a report titled "The top 7 cyber security predictions for 2018" saying "Integration of security technology" would be achieved by adoption of Security Operations and Analytics Platform Architecture (SOAPA). ESG (Enterprise Strategy Group, a renowned integrated IT research, analyst, strategy and validation firm) published a research paper on SOAPA in September, 2017. Study for research paper was commissioned by Mcafee. This research paper described SOAPA as a new model for security operations that knits cyber security tools into a loosely coupled software system. SOAPA is designed to integrate, orchestrate, and automate endpoint protection platforms, endpoint detection/response tools, incident response platforms, network security analytics, user and entity behaviour analytics, vulnerability scanners and security asset managers, anti-malware sandboxes, and threat intelligence. As a dynamic environment, new data sources, applications, and technologies can be added incrementally over time for additional utility. Beyond data exchange between security tools, SOAPA provides centralised command and control for analytics and management of the security infrastructure. Using SOAPA, security analysts can quickly pivot across tools to find data and take action as they need in real time. In the past and till recently organisations are using SIEM (Security Information and Event Management System) system that provides quicker identification, analysis and recovery of security events. SIEM centralises the storage and interpretation of logs and allows near real-time analysis. SIEM collects data into a central repository for trend analysis and provides automated reporting for compliance and centralised reporting. Within SOAPA SIEM has a pivotal role by aggregating analytics data into common repository. SOAPA is an architecture that sits "above and below the SIEM".

SOAPA is designed to integrate, orchestrate, and automate endpoint protection platforms, endpoint detection/response tools, incident response platforms, network security analytics, user and entity behaviour analytics, vulnerability scanners and security asset managers, anti-malware sandboxes, and threat intelligence.

Things like probes and data collectors lie below the SIEM, while advanced analytics and security operations services like user behaviour analytics sit above and can help provide advanced SIEM functionality.

NCIIPC Initiatives

NCIIPC at Meridian Process 2017 (Oslo, Norway)

In 2017 India became the member of Meridian community through participation in the 13th Meridian process held at Oslo, Norway on 24-25 October 2017. The Meridian Process aims to exchange ideas and initiate actions for the cooperation of governmental bodies on Critical Information Infrastructure Protection (CIIP) issues globally. It explores the benefits and opportunities of cooperation between governments and provides an opportunity to share best practices from around the world. The Meridian Process seeks to create a community of senior government policymakers in CIIP by fostering ongoing collaboration. Indian team was led by DG, NCIIPC. He shared the experiences and challenges for Critical Information Infrastructure Protection with other Meridian states.

DG, NCIIPC sharing experiences and challenges for Critical Information Infrastructure Protection with other Member States at Meridian2017

DG, NCIIPC with Team at Meridian2017 representing India

One Day Security Sensitisation Workshop at Chandigarh

Department of Governance Reforms, Punjab in collaboration with NCIIPC organised "One Day Information Security Sensitisation Workshop on Critical Information Infrastructure Protection" on 21st November 2017 at Chandigarh. Sh. Parminder Pal Singh, Director/CISO, Dept. of Governance Reforms, Govt. of Punjab delivered the welcome address. The event was inaugurated by Dr. Nirmaljit Singh Kalsi, Additional Chief Secretary, Govt. of Punjab. He addressed the importance of Critical Information Infrastructure (CII) in our day to day life, followed by the Keynote address by Dr. Ajeet Bajpai, DG, NCIIPC. Sh. Lokesh Garg, Director NCIIPC explained the Roles and Responsibilities of NCIIPC. Sh. Rakesh Kumar, Coordinator (States) elucidated "Cyber Hygiene and Best Practices" to be exercised to safeguard the critical assets. Sh. Navdeep Pal Singh, Sectoral Coordinator (Government) delivered the talks on 'Mapping of Attack Vectors to NCIIPC Control Guidelines v2.0' and "NCIIPC Initiatives and Services". Shri Aniruddha Kumar, Sectoral Coordinator (BFSI) described the Standard Operating Procedures developed by NCIIPC for the CII stakeholders. He also delivered talk on "Framework for Evaluating of Cyber Security for CII".

Participants of One Day Security Sensitisation Workshop at Chandigarh

One Day Security Sensitisation Workshop at Imphal

"One Day Information Security Sensitisation Workshop on Critical information Infrastructure Protection" was jointly organised by NCIIPC and Department of Information Technology, Manipur on 8th September 2017. The event was inaugurated by Shri M. H. Khan, IAS, Principal Secretary (AR/Relief & Disaster Management/ Science & Technology/Fisheries/linked Secretary IT Dept.), Government of Manipur. NCIIPC team was led by Sh. Lokesh Garg, Director NCIIPC along with Sh. Navdeep Pal Singh, Sectoral Coordinator (Government), Shri Neeraj Saini, Sectoral Coordinator (Telecom) and Shri Rakesh Kumar, Coordinator (States).

One Day Security Sensitisation Workshop at Imphal

Shri Rakesh Kumar, Coordinator (States) delivering talk in Sensitisation Workshop at Imphal

NCIIPC in BHEL's Crisis Management Group Meet

Bharat Heavy Electricals Limited (BHEL) organised its Crisis Management Group Meet-V on 21st Dec 2017 at New Delhi. NCIIPC team led by Sh. Sanjeev Chawla, DDG, NCIIPC participated in the event. Sh. Navdeep Pal Singh, NCIIPC delivered a talk on roles and responsibility of NCIIPC, its functions and duties, identification and notification of Critical Information Infrastructure, NCIIPC recommendations and various initiatives like Security Operations Centre, Knowledge Management System, Incident Response, and Responsible Vulnerability Disclosure Program etc.

Sh. Sanjeev Chawla, DDG, NCIIPC at BHEL's Crisis Management Group Meet

Upcoming Events - Global

January 2018

- FloCon 2018, Tucson, Arizona 8-11 Jan
- International Conference on Cyber Security, New York 8-11 Jan
- Real World Crypto 2018, Zurich, Switzerland 10-12 Jan
- Blockchain Cruise Asia, Singapore 15-19 Jan
- Enigma 2018, Santa Clara, California 16-18 Jan
- S4x18, Miami Beach, Florida 16-18 Jan
- ShmooCon, Washington 19-21 Jan
- The Coming-of-Age of Quantum Cybersecurity, Les Diablerets, Switzerland 20-26 Jan
- 4th International Conference on Information Systems Security and Privacy, Madeira, Portugal 22-24 Jan
- Blockchain Protocol Analysis and Security Engineering 2018, Stanford University 24-26 Jan
- PCI London 2018 25 Jan
- AppSec California 28-31 Jan
- NextGen SCADA Europe 2018, Amsterdam, Netherlands 30 Jan-1 Feb

February 2018

- Offensive Security Conference, Berlin, Germany 12-17 Feb
- Pacific Rim Critical Infrastructure Security Summit Honolulu, Hawaii 21-22 Feb
- DevSecCon Singapore 22-23 Feb
- 4th International Conference on Cryptography and Information Security, Dubai, UAE 24-25 Feb
- CSO50 Conference, Scottsdale, Arizona 26-28 Feb
- Financial Cryptography and Data Security Newport, Curacao 26 Feb-2 Mar

March 2018

- PROTECT International Exhibition and Conference on Security & Safety, Manila, Philippines 5-6 Mar
- 2nd Annual FINSEC 2018, Dubai, UAE 5-6 Mar
- 25th International Workshop on Fast Software Encryption, Bruges, Belgium 5-7 Mar
- Cyber Security for Critical Assets, Houston, Texas 6-8 Mar

JANUARY 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			

FEBRUARY 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			

• Security and Policing (Closed 'Government-Level' Cybersecurity Conference), UK	6-8 Mar
• 13th International Conference on Cyber Warfare and Security, Washington	8-9 Mar
• 2nd International Conference on Cryptography, Security and Privacy, Guiyang, China	16-18 Mar
• Black Hat Asia 2018, Singapore	20-23 Mar
• 6th International Symposium on Digital Forensic and Security, Antalya, Turkey	22-25 Mar
• International Conference on Practice and Theory of Public Key Cryptography, Rio De Janeiro, Brazil	25-28 Mar
• Global Privacy Summit 2018, Washington	27-28 Mar
• World Cyber Security Congress 2018, London	27-28 Mar
• Zer0Con, Seoul, South Korea	29-30 Mar

April 2018

• RSA Conference 2018, San Francisco	16-20 Apr

MARCH 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

APRIL 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					

Upcoming Events - India

February 2018

• Cyber Phoenix Conclave 2k18, Jaipur	3-4 Feb
• SANS Secure India 2018, Bangalore	12-17 Feb

March 2018

• Nullcon Security Training, Goa	2-3 Mar
• 2nd Internet of Things India Expo 2018, New Delhi	7-9 Mar

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.