NEWSLETTER

April 2017

National Critical Information Infrastructure Protection Centre

VOLUME 1 ISSUE 2

NCIIPC Newsletter

April 2017

Inside This Issue

More than 700 govt. websites were hacked in last 3 years emphasizing the need for incorporation of cyber security clause in implementation of various govt. projects.

Message from the NCIIPC Desk

We welcome our readers to the second issue of NCIIPC newsletter and hope you must have enjoyed the inaugural issue. The purpose of this newsletter is to disseminate the latest information and happenings related to protection of Critical Information Infrastructure (CII). NCIIPC is continuously working towards identification of national CII and mechanism for its safeguard. NCIIPC has celebrated its 3rd raising day on 16th January 2017. The event was attended by 350 key personnel from government and industry.

In this quarter various cyber-attacks on CII like banking, electricity and oil companies have been observed. There has been incident of attacks on Turkey's Akabank via SWIFT. SWIFT which serves as the back bone for banking transactions worldwide has also been under attack previously. In energy sector, the Ukrainian critical infrastructure was attacked which continued for 4 days and also caused power blackout. There is news of Shamoon 2 hitting again destructively on Saudi Arabian companies. Govt. of India has launched a Cyber Swachhta Kendra for public providing facility to scan phone or computer for malwares. It is important to maintain cyber hygiene and safety with increased use of digital means for banking and other govt. services. More than 700 govt. websites were hacked in last 3 years emphasizing the need for incorporation of cyber security clause in implementation of various govt. projects.

In recent trends, NIST has started inviting proposals for post-quantum crypto algorithms. The current crypto algorithms in use will be easily broken with the advent of quantum computing. It is required that new algorithms are timely developed to maintain the security in quantum era. In other event, researchers from Google have released a tool called Wycheproof for testing crypto libraries. The security not only depends upon the strength of crypto algorithm, it also depends upon its implementation. Heartbleed vulnerability is a recent example for the same.

NCIIPC brings you guidelines for implementation of remote access in Industrial Control Systems. We also present the top ten findings of cyber security preparedness survey jointly conducted by NCIIPC and ISGF. We also provide recommendations or action items required to fill in those gaps.

News Snippets - National

Whether GSTN needs a security clearance?

http://indianexpress.com/article/india/mha-writes-to-finance-ministry-will-pvt-gstn-need-security-clearance-4513141/

The Union Home Ministry has sought a response from the Research and Analysis Wing and the Intelligence Bureau on whether Goods and Services Tax Network (GSTN), the special purpose vehicle set up to provide IT infrastructure and services for implementation of the Goods and Services Tax (GST), needs a security clearance. The Union Ministry has also written to the Finance Ministry to ascertain whether GSTN, a private limited company, is among the sector and category where a security clearance is mandatory from the MHA. The MHA had come out with guidelines for security clearances in May 2015. As part of this, 15 parameters were set in sensitive areas such as defense, telecom, ports, power, civil aviation, up-linking/down linking of TV channels or FM stations, and FIPB (Foreign Investment Promotion Board) proposals. The government owns 49 percent in GSTN, while 51 percent is controlled by private companies, including HDFC, ICICI Bank among others. Some of these private entities are controlled by foreign institutional investors (FIIs), said officials.

51 per cent is controlled by private companies.

Some of these private entities are controlled by foreign institutional investors.

More than 700 Govt. websites hacked between 2013 and 2016

http://timesofindia.indiatimes.com/india/over-700-government-websites-hacked-from-2013-to-2016/articleshow/57029456.cms

Minister of State for Home in parliament informed that more than 700 Govt. websites were hacked between 2013 and 2016. As per information reported to and tracked by the Computer Emergency Response Team (CERT-IN), as many as 199 websites were hacked in 2016, compared to 164 in 2015, 155 in 2014 and 189 in 2013. In a recent cyber-attack, the website of National Security Guard was partially defaced and abusive messages posted on the home page by unknown hackers. Similar cyber-attacks were also reported on websites of ordnance factories and railways. Minister said the govt. had initiated several policy, legal and technical measures such as audit of the systems and networks, increasing awareness in area of cyber security, sharing threat-related information with stakeholders, issuing advisories on such threats through CERT-IN and NCIIPC, and capacity development to address the issue of cyber hacking.

Note: Due to thrust on Digital India initiative and switching of govt. business to ERP, PMS (Project Monitoring System) and centralized databases like Aadhaar etc., there is increase in cyber-attack surfaces resulting in lot of attacks happening on govt. portals.

199 websites were hacked in 2016, compared to 164 in 2015, 155 in 2014 and 189 in 2013

Launch of Cyber Swachhta Kendra

https://90paisa.blogspot.in/2017/02/central-government-introduced-free-anti.html

Minister of Electronics and IT, launched the Cyber Swachhta Kendra–Botnet Cleaning and Malware Analysis Centre for analysis of malware and botnets that affect networks and systems. The Centre is operated by CERT-In. The Hon'ble Minister also made the following announcement:

- The National Cyber Coordination Centre to be operational.
- Sectoral CERTs to be created,
- CERTs to be set up in the state level,
- 10 more STQC facilities to be set up,
- Testing fee for start-up to be reduced by 50 percent.

The Centre will operate in close co-ordination and collaboration with Internet Service Providers (ISP) and Antivirus companies. Whenever an infection is detected, the Centre will send alerts on the infected IP addresses to the ISPs, who in turn will inform the end-user. The Centre will work with banks to detect malware in their network and enable remedial actions. The Centre will provide free tools for detection and removal of malicious programs. The user can log on to www.cyber swachhtakendra.gov.in and clean their systems using the free tools. Users can also educate themselves and get information to secure their computers and mobiles.

The user can log on to www.cyberswachhtakendra.gov.in and clean their systems using the free tools.

Post demonetisation Financial Sector has become most critical

http://telecom.economictimes.indiatimes.com/news/india-sees-surge-in-cyber-crime-incidents-assocham-pwc-study/56646144

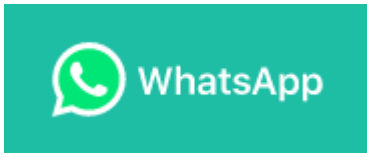
A surge in the cyber security related incidents in India has been noticed with a total of 39730 incidents reported in the first 10 months of 2016 whereas, 44679 and 49455 incidents were reported in 2014 and 2015 respectively. The study, conducted by ASSOCHAM jointly with PwC was released at Workshop on "Securing the Cashless Economy". The return on investments for cyberattacks in India is greater, due to more time taken to detect and respond to cyber-attacks, the study highlighted. The study noted an increase in the number of incidents in banking systems. Highlighting the role of Application Programming Interfaces (APIs), the study pointed out the risk of malware injection through such APIs. "Post demonetisation banking and financial sector has become the most critical. Earlier (cyber) threats were of nuisance value, now they are disruptive and may become destructive," said Dr. Ajeet Bajpai, Director General, NCIIPC.

"Post demonetisation banking and financial sector has become the most critical. Earlier (cyber) threats were of nuisance value, now they are disruptive and may become destructive," said Dr. Ajeet Bajpai, Director General, NCIIPC.

Security personnel alerted against WhatsApp virus

http://economictimes.indiatimes.com/news/defence/defence-security-forces-alerted-against-whatsapp-virus/articleshow/56258702.cms

Central security agencies have alerted security personnel against the malicious activity of a virus, falsely bearing the name of elite organisations like NDA and NIA. An advisory has been issued to the defense and security establishments that the two notorious virus files "NDA-ranked-8th-toughest-College-in-the-world-to-get-into.xls" and "NIA-selection-order-.xls" are circulating over WhatsApp. The advisory added that the corrupt virus files are programmed to illegally extract personal information of the user, their login credentials and banking details like passwords and PIN. Officials said the advisory has now been shared with the field formations of these security forces so that the troops and officers on the ground are made aware and alerted against this virus which has been seen prowling in the instant messaging cyber space. The personnel have also been asked to report these incidents to their Information technology cells, they said. In another similar report released by Lookout and Kaspersky it is revealed that a group of highly talented hackers are spying on the Israeli Defense Force by hacking into the personal smartphones of individual soldiers (https://www.cyberscoop.com/israeli-soldiers-personal-android-phones-hacked-spies-researchers-say/).



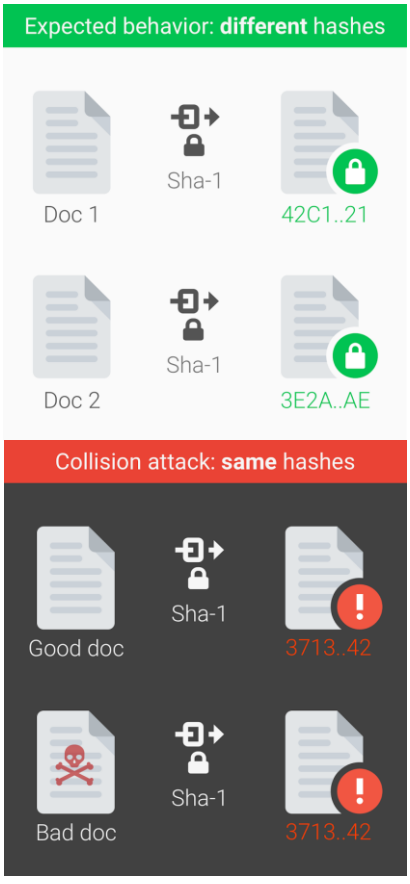
Two notorious virus files "NDA-ranked-8th-toughest-College-in-the-world-to-get-into.xls" and "NIA-selection-order-.xls" are circulating over WhatsApp.

News Snippets - International

The technique for generating a SHA-1 collision has been found

https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

Hashes play a role in browser security, managing code repositories, or detecting duplicate files. Hash functions compress large amounts of data into a small message digest. Finding two messages that lead to same digest should be computationally infeasible. More than 20 years after SHA-1 was introduced, the practical technique for generating a collision has been found. This is culmination of two years of research between CWI Institute and Google. A collision occurs when two distinct pieces of data hash to same digest. In practice, it should never occur for secure hash functions. However, if the hash algorithm has some flaws, a well-funded attacker can craft a collision to deceive systems that rely on hashes into accepting a malicious file in place of its benign counterpart. It's more urgent than ever to migrate to SHA-256 or SHA-3. Following Google's vulnerability disclosure policy, it will wait for 90 days before releasing code that allows anyone to create a pair of PDFs that hash to the same SHA-1 sum.



The attacks began on 16th December and raged for four days.

Wide-ranging attacks on Ukrainian Critical Infrastructure

https://www.theregister.co.uk/2017/01/12/ukraine_power_outtage_hack/

Hackers of unknown origin cut power supplies in Ukraine for a second time in last one year as part of wide-ranging attacks that hit the country in December. The attacks were revealed at the S4x17 conference in Miami. The attacks began on 16th December and raged for four days. Attackers triggered an hour-long power blackout at midnight 17th December by infecting the Pivnichna remote power transmission facility, knocking out remote terminal units and the connected circuit breakers. Further attacks left Ukrainians unable to purchase rail tickets and delayed payments. The attacks also used the BlackEnergy and KillDisk malware. Other hacks included phishing attacks against a Ukrainian bank, various remote exploitation, and DoS attacks. Researcher Oleksii Yasynskyi reckoned that the attackers were a mix of groups specialising in different aspects of offensive security. Hackers kept quiet observation for months whenever one payload was successful at breaching one of the Ukrainian assets, Krotofil told.

There is speculation that this might be retaliation for hacking against Iranian petrochemical facilities.

Saudi government companies hit by attacks from Shamoon 2

http://www.theregister.co.uk/2017/01/26/shamoon_2_hits_saudi_arabian_targets/

At least 15 Saudi govt. offices and companies were hit by another wave of attacks from Shamoon 2 malware. Shamoon surfaced in 2012 when it infected 30,000 workstations in the oil production firm, Saudi Aramco, wiped their hard drives, and put the giant into panic mode. Since then the malware has been refined, and attacks have continued on Saudi govt. and industry targets. Malware is thought to be the creation of state-sponsored hackers. There is speculation that this might be retaliation for hacking against Iranian petrochemical facilities. Between July and September, there was a series of incidents at Iranian facilities, including a fire at the Petrochemical Complex. Head of the Iranian cybersecurity said that, the damage was caused by hacking. Researchers at IBM have cracked the propagation techniques used by the malware. The attacker spam out emails to staff in the target company, impersonating a trusted person and bearing a word document marked as resume. The team also identified two domains used to host malicious executables and carry out attacks. Ntg-sa.com mimics the ntg.sa.com domain of firm Namer Trading Group and maps-modon.club is similar to the maps.modon.gov.sa domain. IBM advises blocking connections to and from these domains and doing a network scan.

Security lapse at a New York International Airport

http://www.zdnet.com/article/unsecured-servers-at-new-york-airport-left-exposed-for-a-year/

A security lapse at a New York international airport left its server backups exposed on the open Internet for almost a year. The Internet-connected storage drive contained several backup images of servers used by Stewart International Airport, but neither the backup drive nor the disk images were password protected, allowing anyone to access their contents. The airport is regularly used by the military and accommodating charter flights. The files contained 11 disk images, which when mounted included airport staff email accounts, sensitive human resources files, interoffice memos, payroll data, and financial tracking database. Many of the files include "confidential" internal airport documents, which contain schematics and details of other core infrastructure. One file contained list of usernames and passwords for various devices and systems, allowing unfettered access to the airport's internal network.

Note: Well defined policy controls need to be implemented for any third party off-shoring of organisation data. To protect security lapse it is highly recommended to encrypt the data (including the back-up servers) with latest encryption standard and suitable access control mechanism.

Image by Daniel Case at the English language Wikipedia, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=3562553

One file contained list of usernames and passwords for various devices and systems.

Hackers targeted Turkey's Akbank via the SWIFT

http://www.reuters.com/article/us-akbank-cyber-idUSKBN1450MC

Hackers targeted Turkey's Akbank via the SWIFT (Society for Worldwide Interbank Financial Telecommunication) global money transfer system in an attack costing up to $4 million. SWIFT, a Belgium-based co-operative owned by both central and commercial banks, said it had "no indication that our network and core messaging services have been compromised". SWIFT operates a messaging network that has been considered reliable in handling trillions of dollars in daily fund transfers. In February 2016, hackers used stolen Bangladesh bank credentials to request the transfer of $1 billion from its correspondent account at the New York Federal Reserve and succeeded in moving $81 million to accounts in Manila. SWIFT in May launched a program to get member banks to comply with cybersecurity guidelines, practice two-factor authentication, and adopt updated SWIFT software.

Note: Recent attacks on SWIFT interface, either by hacking or with co-operation of local bank staff, underscore how its role as the backbone of international banking also presents a risk.

AKBANK

SWIFT operates a secure messaging network that has been considered reliable in handling trillions of dollars in daily fund transfers.

Massive hack in Polish Banks

http://www.theregister.co.uk/2017/02/06/polish_banks_hit_by_malware_sent_through_hacked_financial_regulator/

Polish banks are investigating a massive systems hack after malware was discovered on several workstations. The source of the executables is its own financial regulator, the Polish Financial Supervision Authority (KNF). A spokesman for the KNF confirmed that their internal systems had been compromised by someone "from another country". But when it was discovered that the regulator's servers were hosting malicious files that were then infecting banks' systems, the decision was made to take down the KNF's entire system. The details were rapidly shared between the banks in the country and other banks started reporting the same issues. It is the KNF that sets cybersecurity standards for Polish banks but it is thought that a modified JS file resulted in visitors to the regulator's site loading an external JS file which then pulled down malicious payloads. Both the KNF and the Polish government have told local media that there is no indication that people's money was touched.

A modified JS file resulted in visitors to the regulator's site loading an external JS file which then pulled down malicious payloads.

Dridex v4, the first Banking Trojan to leverage the AtomBombing

https://www.scmagazine.com/new-dridex-borrows-from-atombombing-code-injection-technique-uk-banks-already-targeted/article/641411/

Developers behind Dridex have launched a new version of the banking Trojan, based on a novel technique called AtomBombing. European banks are already feeling the heat from the upgraded malware, according to IBM. AtomBombing is a sneaky technique for injecting code from one process to another. It is designed to eliminate the use of certain telltale API calls (VirtualAllocEx, WriteProcessMemory and CreateRemote Thread) that otherwise might alert detection solutions. Dridex v4 has targeting banks, attempting to hit them with hidden virtual network computing-based RAT attacks and redirection attacks, the IBM report states. Instead of using the aforementioned API calls, AtomBombing instead allows malware to make use of Windows' atom tables and the native API NtQueueApcThread "to copy a payload into a read-write memory space in the target process," IBM explains. "It then uses NtSetContextThread to invoke a return-oriented programming chain that allocates read/write/execute memory, copies payload into it and executes it. Finally, it restores the original context of the hijacked thread."

AtomBombing is a sneaky technique for injecting code from one process to another.

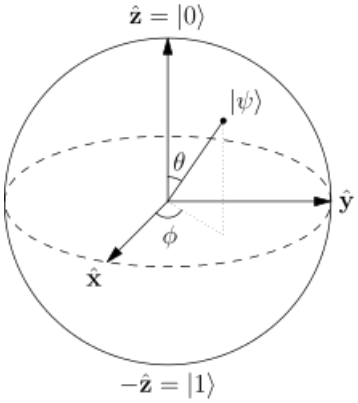
Note: The new Dridex infection uses svchost and spoolsrv to communicate to peers and first-layer command-and-control (C2) servers.

Trends

Proposals invited for post-Quantum Cryptography Algorithms

http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2016-06/2_post-quantum_dmoody.pdf

In recent years, there has been a substantial amount of research on quantum computers. If large-scale quantum computers are built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications. The goal of post-quantum cryptography is to develop crypto systems that are secure against both quantum and classical computers, and can interoperate with existing protocols. Historically, it has taken almost two decades to deploy modern public key cryptography infrastructure. Therefore, regardless of exact time of the arrival of quantum computing era, we must begin now to prepare our systems to be able to resist the same. NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Nominations for candidate algorithms may be submitted by Nov 30.

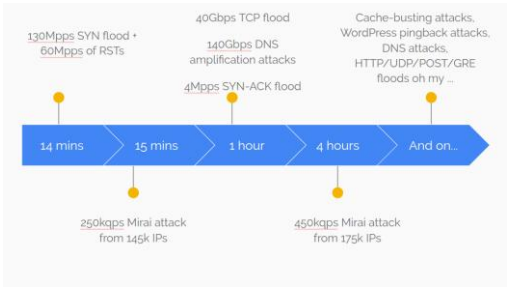


If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use.

Project Shield ultimately brought KrebsOnSecurity back online

https://arstechnica.com/security/2017/02/how-google-fought-back-against-a-crippling-iot-powered-botnet-and-won/

In Sept, KrebsOnSecurity website was on receiving end of the biggest Distributed Denial-of-Service (DDoS) attacks ever recorded. The site soon went dark after Akamai said it would no longer provide the site with free protection. A Google-operated service called Project Shield ultimately brought KrebsOnSecurity back online and has been protecting the site ever since. Once Project Shield ultimately got KrebsOnSecurity back online, it took just 14 minutes for the attacks to resume. The first one came in the form of a flood of 130 million syn packets per second, a volume that's big enough to bring down plenty of sites, but a tiny drop when measured against the resources Google has. About a minute later, the attack shifted to a slightly more powerful flood of about 250,000 HTTP queries per sec. It came from about 145,000 different IP addresses. The attackers followed it with yet more variations, including a 140 Gbps attack made possible through a technique known as DNS amplification and a 4 million packet per-sec syn-ack flood. At the four-hour mark, KrebsOnSecurity experienced one of the bigger attacks seen by Project Shield engineers. It delivered more than 450,000 queries per sec from about 175,000 different IP addresses. Like the attacks that preceded it, it posed no immediate threat to KrebsOnSecurity or the Google resources.



At the four-hour mark, KrebsOnSecurity experienced one of the bigger attacks seen by Project Shield engineers. It delivered more than 450,000 queries per sec from about 175,000 different IP addresses.

Latest Technological Trends for Telecom Industry

Sectoral Coordinator, Telecom

Advancements in telecom have been the primary driver of growth in number of industries across the world. India has emerged as the 2nd largest telecom market in the world. A rapid growth in data consumption and the popularity of mobile apps serve as an indication of the transformation powered by the country's telecom infrastructure. NCIIPC foresee trends for India's telecom sector which also requires the new security aspects to be taken care of.

Rural Broadband service and 4G Expansion: In 2017, we expect telcos to invest more on expanding 4G coverage. Also, Govt. of India's BharatNet project will start ramping up and expected that large parts of rural India will join the Internet revolution.

Trend to 5G: 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.

Digital Payments: The demonetization drive has given a massive push towards digital economy. The recent launch of BHIM app, has contributed for e-transactions over a smartphone.

The Rise of Messaging Apps: With 2G/3G networks, VoIP calls were not very reliable or of good quality. 4G allows a satisfactory quality of a voice call over the Internet which is much cheaper than traditional voice calls. This is causing to use WhatsApp or Skype calls to make phone calls.

Technology Convergence: With the challenge of telecom service providers to support everything from 2G, 3G, 4G, enterprise services and triple play, a converged packet optical network, would make the most sense to reduce expenditure.

Security Aspects: Let's take the latest technology i.e. LTE which was designed to simplify operations and to get lower response times. With elimination of Radio Network Controller in LTE network, the path between user equipment to the core network is more vulnerable to cyber-attack. Therefore, with latest trends in telecom, NCIIPC sees some potential security requirements:

- Platform security requirements
- Confidentiality of user and device identity (including location privacy)
- Entity authentication (Mutual authentication and key agreement between mobiles and the network)
- Security visibility and configurability
- Signaling data confidentiality and integrity
- User data confidentiality (not in LTE: integrity)

With elimination of Radio Network Controller in LTE network, the path between user equipment to the core network is more vulnerable to cyber-attack.

Learning

Guide for Cybersecurity Event Recovery

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

The Framework for Improving Critical Infrastructure Cybersecurity defines five functions: Identify, Protect, Detect, Respond, and Recover. At a more fundamental level, the capabilities in the Recover function have a significant effect across the organization by providing realistic data for improving other capabilities. Effective planning is a critical component of an organization's preparedness for cyber event recovery. Recovery planning enables participants to understand system dependencies; critical personnel identities such as crisis management and incident management roles; arrangements for alternate communication channels, services, and facilities; and many other elements of business continuity. Planning also enables to explore "what if" scenarios, which might be largely, based on recent cyber events that have negatively impacted other organizations, in order to develop customized playbooks. In light of an increasing number of cybersecurity events, organizations can improve resilience by ensuring that their risk management processes include comprehensive recovery planning. Identifying and prioritizing organization resources helps to guide effective plans and realistic test scenarios. This preparation enables rapid recovery from incidents when they occur and helps to minimize the impact on the organization and its constituents. This publication provides tactical and strategic guidance regarding the planning, playbook developing, testing, and improvement of recovery planning.

Planning also enables to explore "what if" scenarios, which might be largely, based on recent cyber events that have negatively impacted other organizations.

The Seven Most Dangerous New Attack Techniques

https://www.sans.org/the-seven-most-dangerous-new-attack-techniques

Which are the most dangerous new attack techniques? What's coming next and how can you prepare? This fast-paced briefing of a keynote session of RSA conference 2017 provides answers from the three SANS top security researchers.

Ransomware: Ransomware combined with crypto currencies are ideal uses of cryptography to benefit the bad guys. Ransomware is highly efficient for attackers, because it requires no command and control channel, no exfiltration, and no contact initiated by the attacker. Instead, the ransomware "customers" reach out to the attacker for "help" recovering from the infection.

Ransomware combined with crypto currencies are ideal uses of cryptography to benefit the bad guys.

With worms spreading to millions of IoT devices, attackers can leverage these systems to create massive floods to take any organization off of the Internet.

The attacks causing power outages in Ukraine were planned and highly coordinated. The attacks left their targets with little confidence in relying on their remaining automation; forcing them to operate in a manual state.

Encryption without good random numbers will put a wide range of security related algorithms at risk.

Internet of Things (IoT) Attacks: Earlier the smart devices, like light bulbs, thermostats, webcams, etc. have been viewed as targets, allowing an attacker to turn on or off. But, increasingly, the IoT is becoming an attack platform rather than just a target. With large-scale, worms spreading to millions of IoT devices, attackers can leverage these systems to create massive floods to take nearly any organization off of the Internet.

Ransomware and IoT Collide: By encrypting configurations and control infrastructures, attackers could hold thermostats, lighting infrastructures etc. for ransom. The threat is even more pronounced in the Industrial IoT, where a factory's ability to manufacture or to provide service could be held hostage.

Industrial Controls Systems Attacks: Recent attacks have not only disrupted the provision of essential service, but they have been punitive by damaging the automation systems that enable their recovery. The attacks causing power outages in Ukraine were planned and highly coordinated. The attacks left their targets with little confidence in relying on their remaining automation; forcing them to operate in a manual state. Future attacks maybe very difficult to recover from causing outages to be measured in days vice hours.

Weak Random Number Generators: Creating good random numbers is a challenging problem. Small devices make it difficult to collect enough random events to initialize the algorithms used to create random numbers. Encryption without good random numbers will put a wide range of security related algorithms at risk. Most wireless protocols rely on good random numbers to encrypt connections. Without good random numbers, these connections are not secure.

Web Services as a Software Component: Developers are no longer limited to using components that are downloaded and installed. Instead they are increasingly relying on remote web services. The reliance on remote services exposes software to new risks. Services need to be carefully authenticated, and data received needs to be validated. Without properly validating those services, and without testing and monitoring the services, these applications are at increasing risk.

Threats against NoSQL Databases: Complex data types like JSON and XML expose new deserialization threats and developers are generally not yet skilled in securing these databases. SANS DShield observes a continuous stream of scans for vulnerable "nosql" databases. Several NoSQL databases have already been compromised. A vulnerable instance of a NoSQL database will be discovered within hours of being exposed to the Internet.

Vulnerability Watch

Vulnerability in Rockwell Automation Logix5000 Controllers

https://tools.cisco.com/security/center/viewAlert.x?alertId=52266

Vulnerability in multiple Rockwell Automation Logix5000 Controllers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a Denial of Service (DoS) condition. The vulnerability is due to improper processing of malformed Common Industrial Protocol (CIP) packets by an affected device. An attacker could exploit this vulnerability by sending a malformed CIP packet to a targeted device. An exploit could trigger a buffer overflow condition that the attacker could use to execute arbitrary code or invoke a nonrecoverable fault, resulting in a DoS condition. To exploit this vulnerability, an attacker may need access to trusted or internal networks to transmit malformed CIP packets. Administrators are advised to apply the appropriate updates and allow only trusted users to have network access. Administrators may consider using IP-based access control lists to allow only trusted systems to access the affected systems. Administrators can protect affected systems from external attacks by using a firewall and monitoring the affected systems.

The vulnerability is due to improper processing of malformed Common Industrial Protocol (CIP) packets by an affected device.

Hard coded key vulnerability in multiple industrial switches

https://tools.cisco.com/security/center/viewAlert.x?alertId=52754

Vulnerability in Red Lion Sixnet-Managed Industrial Switches and AutomationDirect Stride-Managed Ethernet Switches could allow an unauthenticated, remote attacker to take complete control of a targeted device or disrupt communication to cause a denial of service condition. The vulnerability is due to the use of hard-coded HTTP SSL/SSH keys by a targeted device. The vendors have confirmed the vulnerability and released software updates. Administrators are advised to apply the appropriate updates and to monitor the affected systems.

Vulnerability in the Jakarta multipart parser of Apache Struts

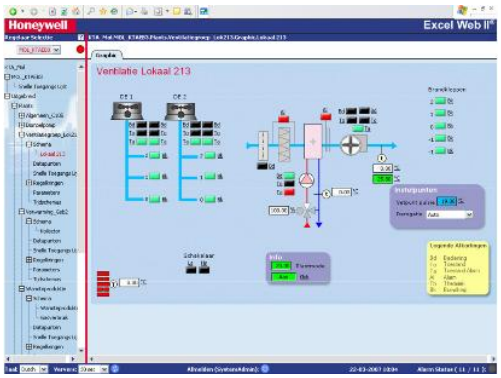
https://tools.cisco.com/security/center/viewAlert.x?alertId=52972

Vulnerability in the Jakarta multipart parser of Apache Struts could allow an unauthenticated, remote attacker to execute arbitrary code on an affected system. The vulnerability is due to improper handling of the Content-Type header value when performing a file upload based on the Jakarta multipart parser of the affected software. An attacker could exploit this vulnerability by persuading a targeted user to upload a malicious file.

Functional code that exploits this vulnerability is publicly available as part of the Metasploit Framework. This vulnerability is actively being exploited in the wild.

Once the Jakarta multipart parser of the affected application uploads the file, the attacker could have the ability to execute arbitrary code. Functional code that exploits this vulnerability is publicly available as part of the Metasploit Framework. This vulnerability is actively being exploited in the wild. Users are encouraged to upgrade to Struts 2.3.32 or Struts 2.5.10.1. Administrators are advised to allow only trusted users to have network access and to monitor affected systems. Administrators may consider implementing a Servlet filter to validate Content-Type header values and to apply Snort SIDs 41818 and 41819 to help prevent attacks that attempt to exploit the vulnerability.

Note: On 6th March, remote code execution vulnerability was reported in Apache Struts 2 (CVE-2017-5638). An advisory to patch the vulnerability has been issued to all the CISOs enrolled with NCIIPC. The official solution provided by Apache suggested either upgrading to a patched version or switching to a different multipart parse implementation (https://cwiki.apache.org/confluence/display/WW/S2-045).



The XL Web II controller application effectively becomes an entry point into the network where it is located.

XL Web II controllers are deployed across Critical Manufacturing, Energy, Water and Wastewater Systems, and others.

Vulnerabilities in Honeywell's XL Web II controller application

https://ics-cert.us-cert.gov/advisories/ICSA-17-033-01

Independent researcher Maxim Rupp has identified vulnerabilities in Honeywell's XL Web II controller application. Password is stored in clear text. An attacker can establish a new user session, without invalidating any existing session identifier, which gives the opportunity to steal authenticated sessions. A user with low privileges is able to open and change the parameters by accessing a specific URL. A user without authenticating can make a directory traversal attack by accessing a specific URL. An attacker with a low skill would be able to exploit these vulnerabilities. These vulnerabilities could be exploited remotely. An attacker may use these vulnerabilities to expose a password by accessing a specific URL. The XL Web II controller application effectively becomes an entry point into the network where it is located. The affected products are web-based SCADA systems. XL Web II controllers are deployed across Critical Manufacturing, Energy, Water and Wastewater Systems, and others. Honeywell has developed Version 3.04.05.05 to fix the vulnerabilities.

Vulnerability in the mail() function in PHPMailer

https://tools.cisco.com/security/center/viewAlert.x?alertId=52233

A vulnerability in the mail() function in PHPMailer could allow an unauthenticated, remote attacker to execute arbitrary commands.

The vulnerability is due to insufficient validation of user-supplied input by the affected software. An attacker could exploit this vulnerability by injecting extra parameters such as a sequence of backslashes (\) to be processed by the mail() function. An exploit could allow the attacker to execute arbitrary code in the security context of the web server user. The vulnerability is due to the passing of extra parameters to the mail command when the Sender property is not set by an affected version of PHPMailer. In addition, the affected software does not take into account the clashing of the escapeshellarg() function with internal escaping with escapeshellcmd() performed by the mail() function on the fifth parameter. This action could allow the attacker to add an extra quote, which could bypass the escapeshellarg() function protection. An exploit of this vulnerability is publicly available. Administrators are advised to apply the appropriate updates and allow only trusted users to have network access. Administrators are also advised to monitor affected systems.

The vulnerability is due to insufficient validation of user-supplied input by the affected software.

Multiple vulnerabilities in Aerospike Database Server

https://tools.cisco.com/security/center/publicationListing.x?resourceIDs=224696&apply=1&totalbox=1&pt0=nonCisco&vd0=224695&sw0=224696&impact=critical#~FilterByProduct

Exploitable stack-based buffer overflow vulnerabilities exist in the querying functionality of Aerospike Database Server 3.10.0.3. A specially crafted packet can cause a stack-based buffer overflow in the function as_sindex__simatch_list_by_set_binid or as_sindex__simatch_by_iname resulting in remote code execution. An attacker can simply connect to the port to trigger this vulnerability. Vulnerability in the RW fabric message particle type and batch transaction field parsing functionality of Aerospike Database Server could allow an unauthenticated, remote attacker to execute arbitrary code. The vulnerability is due to insufficient validation of user-supplied input processed by the server. An attacker could exploit this vulnerability by submitting a crafted packet to the targeted server. Once the affected server processes the crafted packet, the server could fetch a function table outside the bounds of an array or an out-of-bounds write condition could occur, which the attacker could leverage to execute arbitrary code. Aerospike Database Server is both a distributed and scalable NoSQL database that is used as a back-end for scalable web applications that need a key-value store. With a focus on performance, it is multi-threaded and retains its indexes entirely in RAM with the ability to persist data to a solid-state drive or traditional rotational media. Exploit of this vulnerability is publicly available.

Aerospike Database Server is both a distributed and scalable NoSQL database that is used as a back-end for scalable web applications that need a key-value store.

Multiple Vulnerabilities in Advantech WebAccess

https://tools.cisco.com/security/center/publicationListing.x?product=All&title=advantech&impact=critical&sort=-last_published#~Vulnerabilities

Multiple vulnerabilities in Advantech WebAccess could allow an unauthenticated, remote attacker to bypass authentication or conduct attacks. SQL injection vulnerability is due to insufficient validation of user-supplied input by the affected software. The vulnerability exists in the updateTemplate.aspx file. An attacker could exploit the vulnerability by sending crafted SQL queries to the affected software. A successful exploit could allow elevated access to sensitive information. Authentication bypass vulnerability is due to insufficient security restrictions imposed by the affected software. An attacker could exploit this vulnerability by accessing a specific URL on the web server. A successful exploit could allow bypassing authentication and gaining unrestricted access to other pages. To exploit this vulnerability, the attacker may need access to trusted or internal networks to access a specific URL. This access requirement could reduce the likelihood of a successful exploit.

SQL injection vulnerability is due to insufficient validation of user-supplied input by the affected software.

Authentication bypass vulnerability is due to insufficient security restrictions imposed by the affected software.

Note: Towards protection of such software, NCIIPC is sending the advisories and alerts to CIIs organisation on regular basis. Tailored advisories are also being sent to the concerned organisation. Further, on this particular software, NCIIPC has sent the advisories to all constituents. It is always recommended to practice of apply whitelisting rules during configuration of firewall or any security devices to control network access, restrict traffic to specific ports and IP addresses.

Vulnerability in the Tableau Server of the Schneider Electric Wonderware Intelligence software

https://tools.cisco.com/security/center/viewAlert.x?alertId=52969

Vulnerability in the Tableau Server of the Schneider Electric Wonderware Intelligence software could allow an unauthenticated, remote attacker to access sensitive information. The vulnerability is due to improper handling of credentials by the affected system. An attacker could exploit this vulnerability to gain escalated privileges on the host system and to conduct further attacks. To exploit this vulnerability, an attacker may need access to the internal network in which the targeted system resides, making exploitation more difficult in environments that restrict network access. Administrators are advised to apply the appropriate updates and to monitor affected systems. Administrators are also advised to allow only trusted users to have network access and privileged users to access administration or management systems.

An attacker could exploit this vulnerability to gain escalated privileges on the host system and to conduct further attacks.

Vulnerability in Phoenix Contact mGuard

https://tools.cisco.com/security/center/viewAlert.x?alertId=52340

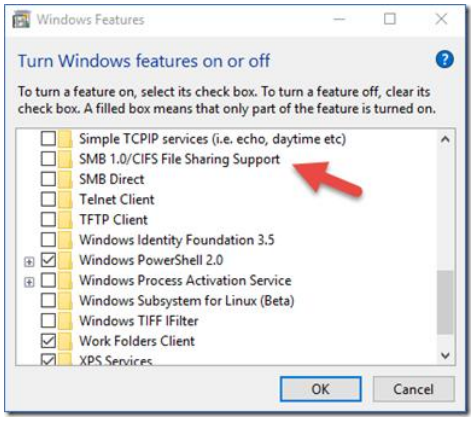
Vulnerability in Phoenix Contact mGuard could allow an unauthenticated, remote attacker to gain elevated privileges on a targeted system. The vulnerability is due to improper password security by the affected software. If the device software has been updated to version 8.4.0, the administrative password may be reset to default password settings. A successful exploit could allow the attacker to log in to the targeted system with elevated privileges. Phoenix Contact confirmed the vulnerability and released software updates. To exploit this vulnerability, the attacker may need access to trusted, internal networks in which the targeted system resides. Administrators are advised to implement a defense-in-depth network security architecture to reduce the risk of unauthorized access to the network in which an affected system resides. Administrators are advised to apply the appropriate updates and to monitor affected systems. Administrators are also advised to allow only trusted users to have network access.

The vulnerability is due to improper password security by the affected software.

Vulnerability in the Microsoft Server Block 1.0 (SMBv1) service

https://tools.cisco.com/security/center/viewAlert.x?alertId=52834

Vulnerability in the Microsoft Server Block 1.0 (SMBv1) service used by multiple Microsoft Windows products could allow an unauthenticated, remote attacker to execute arbitrary code. The vulnerability is due to improper handling of certain requests by the SMBv1 service on an affected system. An attacker could exploit this vulnerability by sending a crafted request to a targeted SMBv1 server. An exploit could allow the attacker to execute arbitrary code. Microsoft confirmed the vulnerability in a security bulletin and released software updates. To exploit this vulnerability, an attacker must be able to send crafted requests to the targeted system. Perimeter filtering devices typically restrict ports such as TCP ports 139 and 445 used for SMB communications, limiting the potential for external attacks. As a result, attackers may require access to internal networks to conduct an exploit. Microsoft has addressed this vulnerability by correcting how the affected software handles crafted requests. Administrators are advised to apply the appropriate updates and to monitor critical systems. Administrators are advised to allow only trusted users to have network access and blocking WAN access to TCP ports 139 and 445 on affected systems in the local network. Administrators may consider using the Microsoft Baseline Security Analyzer (MBSA) scan tool to identify common security misconfigurations and missing security updates on system endpoints.



How to gracefully remove SMB v1 in Windows

Perimeter filtering devices typically restrict ports such as TCP ports 139 and 445 used for SMB communications, limiting the potential for external attacks.

Security App

Project Wycheproof

https://github.com/google/wycheproof

It is developed and maintained by members of Google Security Team, but it is not an official Google product.

It has found that the private key of widely-used DSA and ECDHC implementations can be recovered.

Project Wycheproof tests crypto libraries against known attacks. It is named after Mount Wycheproof, the smallest mountain in the world. The main motivation for the project is to have a goal that is achievable. The smaller the mountain the more likely it is to be able to climb it. It is developed and maintained by members of Google Security Team, but it is not an official Google product. Project Wycheproof provides tests for most cryptographic algorithms, including RSA, elliptic curve crypto and authenticated encryption. The tests detect whether a library is vulnerable to many attacks, including Invalid curve attacks, biased nonces in digital signature schemes, all Bleichenbacher's attacks, and many more. It has over 80 test cases covering more than 40 bugs. It has found that the private key of widely-used DSA and ECDHC implementations can be recovered. Project Wycheproof is by no means complete. Passing the tests does not imply that the library is secure; it just means that it is not vulnerable to the attacks that Project Wycheproof tests for. Developers and users now can check their libraries against a large number of known attacks, without having to spend years reading academic papers or become cryptographers themselves.

CIRCLean is an independent hardware solution to clean documents from untrusted (obtained) USB keys / USB sticks.

CIRCLean hardware solution to clean documents from untrusted USB sticks

https://n0where.net/usb-key-cleaner-circlean/?

Malware regularly uses USB sticks to infect victims, and the abuse of USB sticks is a common vector of infection. CIRCLean is an independent hardware solution to clean documents from untrusted (obtained) USB keys / USB sticks. The device automatically converts untrusted documents into a readable but disarmed format and stores these clean files on a trusted (user owned) USB key/stick. The code runs on a Raspberry Pi (a small hardware device), which also means it is not required to plug the original USB key into a computer. CIRCLean can be seen as a kind of air gap between the untrusted USB key and your operational computer. CIRCLean does not require any technical prerequisites of any kind and can be used by anyone. CIRCLean is free software which can be audited and analyzed by third-parties. CIRCLean is currently tested to work with USB keys that have FAT32, NTFS, or ext2/3/4 filesystems.

NCIIPC Snippets

Protection Strategy for Remote Access in Control Systems

Sectoral Coordinator, Transport

Various organisations are including remote access for SCADA/ICS systems for patch management, updates and health-checkup etc. The remote monitoring through OEMs should be avoided. The possibility should be explored for setting up the facility locally. If the requirement is unavoidable then a proper risk assessment must be done and senior management should be apprised of the risks involved. Security Level SLA should be established with the OEM. Following generic protection strategy may be helpful for remote access in control systems:

- Policy should include SCADA/ICS security controls with exceptional clause included.
- Any configuration changes should lead to risk assessment process and mitigation with suitable controls, if not possible technologically then certain controls may be applied.
- If remote access has to be provided it should be in a controlled environment with multi-factor authorisation. The access must be with least possible time window.
- Separate VPN connection for control system network access. Encrypt all data in transit outside the enterprise.
- Close unused ports. The ports opened should be closed after usage. Untrusted hosts should not be allowed to access.
- Once the endpoints have been authenticated, their security must be assessed before access to control system.
- Patch and update management with staging mechanism.
- Intrusion monitoring and event monitoring applications to supervise the remote sessions, and generate alerts.
- Remote host should meet the requirements of nodes with which it can communicate on trusted control system networks.
- Remote user should be restricted in the scope of hosts with whom they can communicate.
- Separate incident response & forensics for ICS systems and ability to quickly revoke access in case of any incident.
- Completely isolate the remote client from other networks.
- Implementing firewall in "series" from different vendor.
- Any remote access needs to be carried out by trained manpower. If handled by third party it must be for shortest period, considering organisational manpower will takeover to handle such process.

The remote monitoring through OEMs should be avoided.

Security Level SLA should be established with the OEM.

Close unused ports.

The ports opened should be closed after usage.

Untrusted hosts should not be allowed to access the network.

Encrypt all data in transit outside the enterprise.

Completely isolate the remote client from other networks.

Organisations must take steps towards formulation of comprehensive Information Security Policy.

Regular internal and external audit for the cyber security must be conducted.

Organisations must undertake thorough V/T/R

Mechanism for evaluating and approving residual Information Security risk

Cyber Security Preparedness Survey

Sectoral Coordinator, Power & Energy

NCIIPC and India Smart Grid Forum undertook a survey of the information security posture of a sample of the Generation, Transmission & Distribution utilities in order to understand the present status and gaps. Following are the top 10 findings and recommendations of Cyber Security Preparedness Survey to be implemented across all the Critical Sectors.

- *Finding: Many organisations do not have formal Information Security Policy.*

Recommendation: Organisations must take steps towards formulation of comprehensive Information Security Policy. Sub-policies and procedures specific to key operational areas should also be prepared. Organisation needs to establish a formal mechanism by which all stakeholders (Employees, Contractors etc.) are required to read and acknowledge the relevant portions of the relevant policies.

- *Finding: Many organisations do not have an independent Information Security Audit mechanism.*

Recommendation: Regular internal and external cyber security audit must be conducted. The auditors must be considered to be changed on regular intervals.

- *Finding: Organisations are yet to undertake a detailed Vulnerability/Threat/Risk (VTR) analysis of their Critical Information Infrastructure (CII) and necessary measures to address the same. At present, this is being done as an ad-hoc approach in most of the organisations.*

Recommendation: It is essential that CII organisations must undertake thorough V/T/R. Organisations should identify CII and corresponding incoming and outgoing dependencies. Process of obtaining approval for CII notification needs to be initiated.

- *Finding: Risk assessment & mitigation process are yet to be established and/or reviewed regularly by many organisations. The acceptable residual risks are also to be clearly evaluated and business continuity plan need to be appropriately tuned.*

Recommendation: It is essential that a mechanism for evaluating residual Information Security risk be involved in a manner similar to Financial or Operational risk. It is imperative that Information Security risk be owned by organizations.

- *Finding: Organisations are having ad-hoc Cyber Security Incident handling mechanisms.*

Recommendation: Incident management procedures need to be augmented. Some indicative suggestions are:

  - Organisations should undertake regular security awareness training for its employees.
  - Incident management processes must be clearly spelled out with responsibilities of individuals and steps for orderly response to a security incident.
  - Incident management drills.
  - Sensitisation of users and basic training to understand and implement good cyber hygiene.

- *Finding: Automated mechanisms for monitoring inbound and outbound traffic for malicious/unauthorised activities have not been implemented.*

Recommendation: Monitoring of inbound and outbound communications is required to observe for unusual or unauthorized activities. Automated mechanism may be implemented for monitoring inbound and outbound traffic, as they provide effective monitoring. It is also recommended that documentation for the monitoring process may be maintained.

- *Finding: For disposing Critical Digital Assets (CDA), they are simply forwarded to Waste Management companies. Mechanisms for ensuring data leak prevention for CDA have not been considered.*

Recommendation: In order to ensure that no data is inadvertently leaked, policies for disposal of CDA must be formulated. Physical destruction of CDA may be considered as a part of organisation's disposal process.

- *Finding: Organisations do not have strict control over usage of portable devices such as USB media, Mobile phones etc.*

Recommendation: Organisations must define proper usage, access control and security procedure/guidelines for mobile phones/smart-phones and portable media, as they are amongst the foremost source of malware infection and system compromise. They may also adopt the procedure for blocking the unauthorized removable media (e.g. USB device) on systems.

Organisations should undertake regular security awareness training for its employees.

Monitoring of inbound and outbound communications is required to observe for unusual or unauthorized activities.

Physical destruction of CDA may be considered as a part of organisation's disposal process.

Organisations must define proper usage, access control and security Procedure/guidelines for mobile phones/smart-phones and portable media.

Adopt the procedure for blocking the unauthorized removable media.

Organisations must have IT security SLAs with outside agencies.

System hardening may also be included in procurement standards of the organisation.

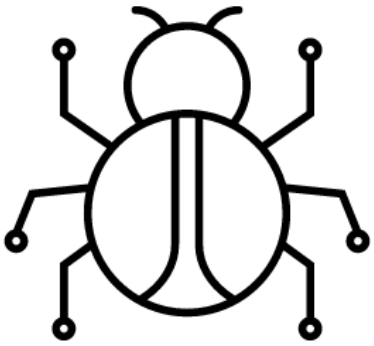
- *Finding:*
  - *Organisations do not have IT security SLA (Service Level Agreement).*
  - *Procurement standards do not include system hardening.*

Recommendation:

- Organisations must have IT security SLAs with outside agencies. This will enforce the other organisations to consider security with the services they are providing.
- System hardening may also be included in procurement standards of the organisation. It will help in making system secure by design.

- *Finding: Many organisations do not conduct Information security awareness trainings.*

Recommendation: Organisations should undertake regular security awareness training for its employees. Effectiveness of security awareness training needs to be reviewed at least once in a year. Practical exercises may be included in the security awareness training that simulates actual cyber-attacks.



103.236.220.38
China, Guizhou, Guiyang
26.583330, 106.716670 (26°34'60"N 106°43'0"E)
Los Angeles USA

Source: ip2location.com

Most Prevalent Malware Files

Following are the most prevalent malware files detected by NCIIPC. The advisories specific to these malwares is periodically pushed to all the CISOs enrolled with NCIIPC.

SHA 256:
81dc8b0b09846fed4dd4d80350bd17d08f21546c873ae4c0aba41b72c572e0fa

MD5: 846CB642B5B8DB10381F158865109EEE

Typical Filename: 3932

Detection Name: Trojan.Linux

Command and Control IP: 103.236.220.38

VirusTotal Link:

https://www.virustotal.com/en/file/81dc8b0b09846fed4dd4d80350bd17d08f21546c873ae4c0aba41b72c572e0fa/analysis

SHA 256:
e859f27fb6dae61764c1c949108fdc0aab5f5226f8a4dc0777bb492ec570864e

MD5: 16e62ee8ca4ed8a5d9f3b878671dd9bf

Typical Filename: a.exe

Detection Name: Trojan.Win32

VirusTotal Link:

https://www.virustotal.com/en/file/e859f27fb6dae61764c1c949108fdc0aab5f5226f8a4dc0777bb492ec570864e/analysis

SHA 256: a4fd47d32cc5b45466039d25e3b5bea680cbcbbfa93f92d8a2561db567f530be

MD5: 238aaed799b45da3f032781d494ff3ab

Typical Filename: bash

Detection Name: Backdoor.Linux

Command and Control IP: 115.236.92.99

VirusTotal Link:

https://www.virustotal.com/en/file/a4fd47d32cc5b45466039d25e3b5bea680cbcbbfa93f92d8a2561db567f530be/analysis

Source: ip2location.com

SHA 256: a6febcd6f857ed906a71a42ea2741869d7cbca217db2db438c3cc929a1897b20

MD5: 238aaed799b45da3f032781d494ff3ab

Typical Filename: Linu

Detection Name: Linux/Dofloo

Command and Control IP: 183.60.149.199

VirusTotal Link:

https://www.virustotal.com/en/file/a6febcd6f857ed906a71a42ea2741869d7cbca217db2db438c3cc929a1897b20/analysis

Source: ip2location.com

SHA 256: a0d9cab10f396e88f064d73002b447074b8ea199bbf3b1e512fa129405ac6c95

MD5: e51fa79d0d0c9d3383d9553c62bfbd4b

Typical Filename: lsxm.7

Detection Name: Trojan.Unix

Command and Control IP: 61.160.213.49

VirusTotal Link:

https://www.virustotal.com/en/file/a0d9cab10f396e88f064d73002b447074b8ea199bbf3b1e512fa129405ac6c95/analysis

Source: ip2location.com

Most Prevalent Malicious Domains

Following are the most prevalent domains used as malware droppers detected by NCIIPC. These domains are usually loaded with malicious binaries used by the malicious files to compromise the system.

By using these malware droppers malicious files have the advantage of being light since entire backdoor need not to be packaged in single malware.

www.linuxhoumen.com

gui4.zhuabtc.com

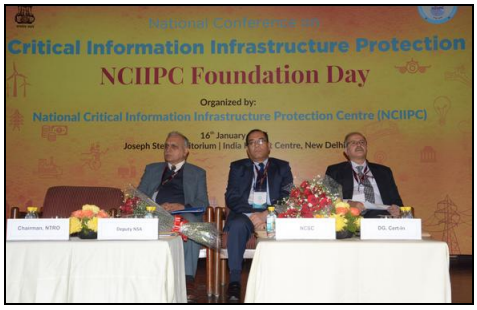
http://45.35.52.178:8552/

http://115.236.92.99:8846/

www.anxinkz.com

yangji.zhuabtc.com

NCIIPC recommends blocking of the malicious files and domains at the perimeter of the network for the protection of critical information assets.



From left to right: Deputy NSA Dr. Arvind Gupta; National Cyber Security Coordinator, Dr. Gulshan Rai; DG CERT-In, Dr. Sanjay Bahl

Chairman, NTRO, Sh. Alok Joshi delivered the Welcome address

Panel discussion

NCIIPC Foundation Day

NCIIPC celebrated its 3rd Foundation Day on 16th January 2017 at India Habitat Centre, New Delhi. NCIIPC was notified as the nodal agency under Section 70A of the IT Act in respect of Critical Information Infrastructure (CII) Protection vide Gazette of India notification on 16th January 2014. The Deputy National Security Advisor, Dr. Arvind Gupta, was the Chief Guest at the event. Chairman, NTRO, Sh. Alok Joshi delivered the welcome address and keynote addresses were delivered by the National Cyber Security Coordinator, Dr. Gulshan Rai, and Director General CERT-In, Dr. Sanjay Bahl. The conference was attended by key policy makers from the government, CII Stakeholders from the Private and Public Industry and a cross section of Cyber Security practitioners. The event aimed to provide a platform for all stakeholders of the CII ecosystem to converge, deliberate and formalize action plans for optimizing and improving protection of the vast array of CII deployed across the nation. The following expert panel discussions were held on the day:

- Way Ahead and Optimisation
- Experience, Views and Expectation of the Industry
- Challenges to and for a Protected System

NCIIPC Initiatives

NCIIPC at IDRBT CISO Forum

Sectoral Coordinator, BFSI

A Chief Information Security Officer (CISO) forum was organized by Institute for Development and Research in Banking Technology (IDRBT) on 6th March 2017, in Hyderabad. The meeting was attended by more than 30 CISOs of the banking sector. Dr. A. S. Ramasastri, Director, IDRBT delivered the inaugural speech. Sh. Aniruddha Kumar, Sectoral Coordinator – BFSI (Banking, Finance and Insurance), NCIIPC, gave a presentation on the initiatives taken by NCIIPC for BFSI sector. The presentation was followed by an interactive session, on role of NCIIPC and expectations from the stakeholders. It is believed that this meeting would result in coherent approach from all the stakeholders in identifying criticality in BFSI Sector for protection. Further, IDRBT officials have shown interest in working on R&D in "Identification & Protection of CII in BFSI Sector". This is an active & significant area of collaboration.

Sh. Jayesh Ranjan, Principal Secretary (IT&C), Govt. of Telangana

Cyber Security Sensitization Workshop for Telangana State

Sectoral Coordinator, States (South Zone)

Telangana State Information Technology, Electronics and Communication Department (IT&C) in collaboration with NCIIPC organized a one day Cyber Security Sensitization Workshop at Haritha Plaza, Begumpet, Hyderabad on 10th February 2017. Over 180 participants from more than eighty departments of Telangana State participated in the workshop. Sh. Jayesh Ranjan, Principal Secretary (IT&C), Govt. of Telangana delivered the keynote address. He explained that Telangana Government has framed a Cyber Security Policy for the state. Sh. Aniruddha Kumar, Sectoral Coordinator, States (South Zone) explained the vision, mission, mandate and functions of NCIIPC. He also elucidated the Critical Infrastructure (CI), Critical Information Infrastructure (CII), threats & challenges to CII and expectations from CII stakeholders. He emphasized on the nomination of Chief Information Security Officer (CISO) for the State and its stakeholders. The necessity of identification and notification of CII was elucidated to the participating organizations of the state. Sh. Navdeep Pal Singh, Sectoral Coordinator, NCIIPC delivered the presentation on 'Mapping of Attack Vectors to NCIIPC Control Guidelines'. Sh. Rakesh Kumar, Sectoral Coordinator, NCIIPC delivered the lectures on 'Cyber Hygiene' and 'Identification and Notification of CII'. In addition to the above, an interactive session was also organized for the participants. The workshop was well received by the participants.

Sh. Navdeep Pal Singh, Sectoral Coordinator

Sh. Aniruddha Kumar, Sectoral Coordinator

Upcoming Events

APRIL 2017

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						

MAY 2017

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			

JUNE 2017

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	

JULY 2017

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 2017

- International Conference on Cyber Security, Cyber Welfare and Digital Forensic, Ethiopia — 22-24 Apr

May 2017

- SC Media RiskSec NY 2017, New York — 2 May
- OWASP AppSec Eurpoe 2017, Belfast — 8-12 May
- International Conference on Cryptography, Coding and Information Security, Amsterdam — 14-15 May
- International Conference on Network and Cyber Security, Lakeland — 19-23 May
- IEEE Symposium on Security and Privacy, San Jose — 22-24 May
- Social Engineering Conference 2017, Jersey City — 25 May
- International Conference on Security And it's Applications, Vienna — 27-28 May

June 2017

- Techno Security & Digital Forensics Conference, Myrtle Beach — 4-7 Jun
- SC Congress, Toronto — 12-13 Jun
- International Conference on Cryptography and Information Security, Zurich — 24-25 Jun
- International Conference on Information Security and Cyber Forensics, Slovakia — 29 Jun-1 Jul

July 2017

- International Symposium on Engineering Secure Software and Systems, Bonn — 3-5 Jul
- International Conference on Digital Security and Forensics, Kuala Lumpur — 11-13 Jul
- Black Hat USA 2017, Las Vegas — 22-27 Jul
- IEEE International Conference on Smart Grid and Smart Cities, Singapore — 23-26 Jul
- RSA Conference 2017 Asia Pacific & Japan, Singapore — 26-28 Jul
- DEF CON 25, Las Vegas — 27-30 Jul

August 2017

- International Conference on Cyber Security, Kota — 12-13 Aug
- International Workshop on Networks and Information Security, Taichung — 13-16 Aug
- USENIX Security Symposium, Vancouver — 16-18 Aug

September 2017

- OWASP AppSec USA 2017, Orlando — 19-22 Sep
- International Conference on Cyber-Security in Aviation, Computer Science and Electrical Engineering, Grand Forks — 21-23 Sep

October 2017

- Virus Bulletin International Conference, Madrid — 4-6 Oct
- ISSA International Conference, San Diego — 9-11 Oct

AUGUST 2017

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

SEPTEMBER 2017

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

OCTOBER 2017

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				

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.