NEWSLETTER

January 2019

National Critical Information Infrastructure Protection Centre

VOLUME 3 ISSUE 1

@NCIIPC

NCIIPC Newsletter

January 2019

स्वच्छ भारत

एक कदम स्वच्छता की ओर

Inside This Issue

Message from the NCIIPC Desk

NCIIPC wishes its readers a very happy, prosperous and cyber secure 2019. With this issue, NCIIPC Newsletter has completed an eventful two-year journey. It is heartening to note the sharp increase in readership and downloads across the globe from over 30 countries. Based on feedback from readers, we are introducing a new section on Mobile Security starting this issue.

The New Year also marks completion of 5 years of NCIIPC. It was on 16th January 2014 when Government of India notified the creation of NCIIPC under section 70A of Information Technology Act 2000.

The security of Critical Information Infrastructure has become a global concern in view of growing cyber threats. On 16 November 2018, USA formalised the Cybersecurity and Infrastructure Security Agency Act of 2018 and established the Cybersecurity and Infrastructure Security Agency (CISA) as a part of ongoing effort to defend the critical infrastructure against the threats of today, while working with partners across all levels of government and the private sector to secure against the evolving risks of tomorrow. In another move, around 57 countries endorsed the Paris Call for Trust and Security in Cyberspace on 12 November 2018. This declaration focuses on developing common principles for securing cyberspace.

At the national level, Government of Andhra Pradesh launched a dedicated web portal for creating cyber security awareness and reporting of cyber security incidents with an objective to reduce the time gap between threat identification and its mitigation. The Ministry of Home Affairs launched a Twitter handle @CyberDost to create public awareness about cyber hygiene and best practices.

Comments, suggestions and feedback are solicited from the readers. It would go a long way towards enhancing the content of subsequent issues. You can write to us at newsletter@nciipc.gov.in

The New Year also marks completion of 5 years of NCIIPC. It was on 16th January 2014 when Government of India notified the creation of NCIIPC under section 70A of Information Technology Act 2000.

News Snippets - National

India-Morocco MoU's on Space Cooperation and Cyber Security

Source: https://spacewatch.global

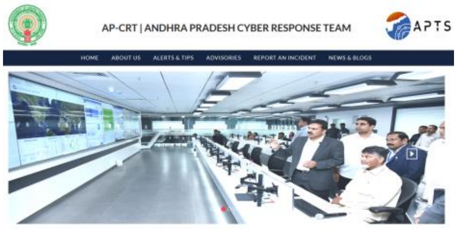
India and Morocco signed Memorandum of Understanding (MoU) on space and cyber security cooperation in New Delhi on 25th September 2018. In 2015 both countries decided to elevate bilateral ties to a strategic partnership and have been working to include new areas of cooperation to the partnership including space and military cooperation as well as traditional economic cooperation. Two bilateral MoU's covering 'Cooperation in Peaceful Uses of Outer Space' between the Indian Space Research Organisation (ISRO) and the Moroccan Centre of Remote Sensing, and Cooperation in the area of Cyber Security between Indian Computer Emergency Response Team (CERT – IN), and the Moroccan Computer Response Team (ma-CERT), were signed in presence of defence ministers of both the countries.

Cooperation in the area of Cyber Security between Indian Computer Emergency Response Team (CERT –IN), and the Moroccan Computer Response Team (ma-CERT)

Andhra Pradesh Launched Web Portal to Combat Cyber Threats

Source: www.newindianexpress.com

The Government of Andhra Pradesh has launched the Andhra Pradesh Cybersecurity Response Team (APCRT), a web portal to provide security from cyber threats. The APCRT, which works on the lines of the Indian Computer Emergency Response Team (ICERT), will extend cybersecurity cover to all the government departments and state-owned entities. With this, AP becomes one of the states in the country to have an exclusive web portal for reporting cybersecurity-related incidents. APCRT functions round-the-clock and incidents can be reported to https://apcrt.ap.gov.in. "The objective is to reduce the time required to mitigate the threat identified from the time it is first reported. The response team works by consolidating the functions of incident monitoring, detection, response, coordination and computer network defence. It also generates cyber threat intelligence and provides cyber threat reporting and advisories for the citizens," a senior official from Andhra Pradesh Technology Services Limited (APTS) said. The APCRT operates from the AP Cyber Security Operations Centre (APCSOC) inaugurated in Vijayawada last year.



APCRT functions round-the-clock and incidents can be reported to https://apcrt.ap.gov.in

Cyber Dost

@CyberDost

cybercrime.gov.in Cyber-safety and Cybersecurity awareness handle maintained by Ministry of Home Affairs, Government of India

@CyberDost for Spreading Awareness about Cybercrimes

https://twitter.com/CyberDost

Information and communication technology is being used in all walks of public life including banking, transport, airlines, railways, power and other sectors. With enhanced use of technology for day to day activities, possibility of cybercrimes is also increasing. Due to lack of awareness about the modus operandi of cybercrimes, some people become victims of various crimes. Education and awareness will help in preventing such crimes to a significant extent. To mitigate possibility of disruption in normal business activities or losses due to cybercrimes, Government of India is committed to create an ecosystem to prevent and control cybercrimes. 'Capacity building' and 'Public awareness' are critical components for obviating impact of cybercrimes and creating a suitable climate for trust-based transactions. With an objective of spreading awareness about cybercrimes and normal precautions to be taken, the Ministry of Home Affairs has launched @CyberDost twitter handle where pertinent posts are being placed regularly. General Public and Government employees will be immensely benefitted if they follow this twitter handle. This will enhance their basic knowledge about cybercrimes and precautions to be taken for prevention thereof.

General Public and Government employees will be immensely benefitted if they follow this twitter handle.

News Snippets - International

Paris Call for Trust and Security in Cyberspace

Source: https://www.diplomatie.gouv.fr

French President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace at the UNESCO Internet Governance Forum on November 12. This high-level declaration on developing common principles for securing cyberspace received the backing of around 57 States including UK, Canada, Australia, Italy and Japan as well as private companies like Microsoft, Google, Facebook, Intel, HP etc. and civil society organizations. Cyberspace, which is becoming increasingly essential to our lives, is a place of opportunity, as well as new threats. The rapid growth in cybercrime and malicious activity poses greater dangers to both our private data and certain critical infrastructures. In order to respect people's rights and provide them safe and secure cyber space, international community must work together, but also collaborate with private-sector partners, the world of research and civil society. Supporters of the Paris Call are committed to working together to:

- Increase prevention against and resilience to malicious online activity;

This high-level declaration on developing common principles for securing cyberspace received the backing of around 57 States including UK, Canada, Australia, Italy and Japan

- Protect the accessibility and integrity of the Internet;
- Cooperate in order to prevent interference in electoral processes;
- Work together to combat intellectual property violations via the Internet;
- Prevent the proliferation of malicious online programmes and techniques;
- Improve the security of digital products and services as well as everybody's 'cyber hygiene';
- Clamp down on online mercenary activities and offensive action by non-state actors;
- Work together to strengthen the relevant international standards.

Work together to strengthen the relevant international standards

Israel among the Providers of Cybersecurity to the G20 Meeting

Source: https://jewishnews.timesofisrael.com/

Israel was among the providers of cyber defence and cybersecurity to the G20 meeting that concluded on 1st December 2018 at Buenos Aires. The Defence Ministry of Argentina signed a contract worth more than $5 million with its Israeli counterpart to provide the cyber defence and cybersecurity services to the meeting. The contract was for the implementation of a Cyber Defence Informatics Emergency Response Team (CERT) and a Computer Security Incident Response Team (CSIRT). The cyber defence program included the capability to inhibit drones to a certain range of action. The cybersecurity software included the ability to collect and analyse information from social networks. The G20 is an international forum for the governments and central bank governors from Argentina, Australia, Brazil, Canada, China, the European Union, France, Germany, India, Indonesia, Italy, Japan, Mexico, Russia, Saudi Arabia, South Africa, South Korea, Turkey, the United Kingdom and the United States. Israel is not a member of the G20 group.

Federal Police motorcycle with G20 logo, Reuters

The cyber defence program included the capability to inhibit drones to a certain range of action. The cybersecurity software included the ability to collect and analyse information from social networks.

Previously Unobserved Threat Actor Targeting Pakistani Officials

Source: www.cyberscoop.com

A previously unobserved threat actor with the characteristics of a nation-state is using advanced techniques to target Pakistani officials connected to the military or government agencies, according to a report published by cybersecurity company Cylance.

Through a combination of old and new methods, the perpetrators, which Cylance labels "White Company," try to deploy spyware onto their victims' systems while avoiding detection. Cylance said that White Company's sophisticated methods of compromise, its evasion techniques and its targets suggest that it's a previously unseen threat actor and is likely state-sponsored. The report breaks down the espionage campaign into two phases. Phase one entails a phishing campaign in which 30 malicious text documents are circulated to targets that are in or have some connection to the Pakistani military. If opened, the documents would execute a shellcode that would cause actual malware to be downloaded from an external source. Those external sources were legitimate Pakistani websites, the researchers say. That means the websites were likely compromised and their domains were unknowingly being used to host White Company's malware.

Phase one entails a phishing campaign in which 30 malicious text documents are circulated to targets that are in or have some connection to the Pakistani military.

Bristol Airport in UK Recovered from a Ransomware Attack

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

The screens at the airport stopped working, Sammer Tang

The Bristol airport in the UK recovered from a ransomware attack which prompted the airport to take flight information screens offline for two days in an effort to keep the attack contained. "We believe there was an online attempt to target part of our administrative systems and that required us to take a number of applications offline as a precautionary measure, including the one that provides our data for flight information screens," airport Spokesman James Gore told. "That was done to contain the problem and avoid any further impact on more critical systems." Gore added that they believe the attack was a speculative attempt and not a targeted attack and that neither flights, security, nor passenger safety was at risk as a result of the attack. The airport was forced to resort to contingency measures in which flight information was handwritten on whiteboards and sheets of paper.

"There was an online attempt to target part of our administrative systems and that required us to take a number of applications offline as a precautionary measure"

Critical Vulnerability in eID Cards System used by Germany

Source: www.zdnet.com

Image: Bund.de

Security researchers from SEC Consult found a critical vulnerability in backbone of the electronic ID (eID) cards system used by the German state. The vulnerability, when exploited, allowed an attacker to trick an online website and spoof the identity of another German citizen when using the eID authentication option. Germany patched a key "e-government" service against possible impersonation attacks, and both private and public sector developers were told to check their logs for evidence of exploits. In July, SEC Consult warned the country's federal computer emergency team at CERT-Bund that software supporting the government's nPA ID card had a critical vulnerability.

Phishing Campaigns Targeting Financial Institutions of Russia

Source: www.spamfighter.com

As per a cyber security firm, two major phishing email campaigns were identified that targeted financial institutions of Russia. The phishing emails were disguised to have come from Russia's financial cyber security authorities and the Central Bank. As per a report by Group-IB based out in Moscow, numerous Russian banks received phishing emails which claimed to have come from the CBR (Central Bank of Russia) on November 15, 2018. The emails that were sent came along with the malicious attachments having a tool that is used by Silence hacker group. Though the attachments in the emails were having an extension of .zip that is actually known to be "the standardization of the format of CBR's electronic communications", however they were the Silence downloader actually.

The phishing emails are disguised to have come from Russia's financial cyber security authorities and the Central Bank.

CISA is Responsible for Protecting the US Critical Infrastructure

Source: www.us-cert.gov

On November 16, 2018, the US President signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018. This Act elevated the mission of the former Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) and established the Cybersecurity and Infrastructure Security Agency (CISA). CISA is responsible for protecting the United States critical infrastructure from physical and cyber threats, a mission that requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

CISA is responsible for protecting the United States critical infrastructure from physical and cyber threats

Trends

Intel's New 9th Generation CPUs Include Hardware Protection for Spectre and Meltdown

Source: www.bleepingcomputer.com

As part of Intel's Fall Desktop Launch event, the new 9th generation CPUs were announced that included hardware protection for two of the Spectre and Meltdown vulnerability variants. The new desktop processors include protections for the security vulnerabilities commonly referred to as 'Spectre', 'Meltdown' and 'L1TF'. These protections include a combination of the hardware design changes announced earlier this year as well as software and microcode updates as below:

- Speculative side channel variant Spectre V2 (Branch Target Injection) = Microcode + Software

Information was slipped into the fine print of a slide announcing the release of Intel's new 9th Gen CPUs

- Speculative side channel variant Meltdown V3 (Rogue Data Cache Load) = Hardware
- Speculative side channel variant Meltdown V3a (Rogue System Register Read) = Microcode
- Speculative side channel variant V4 (Speculative Store Bypass) = Microcode + Software
- Speculative side channel variant L1 Terminal Fault = Hardware

Hardware protection for the L1 Terminal Fault and Meltdown V3 vulnerabilities has been added, but the other vulnerabilities still require software and microcode protection

In March 2018, Intel announced that they would be adding hardware protection to forthcoming CPUs that would protect users against some of the variants through partitioning. With the release of the 9th gen CPUs, hardware protection for the L1 Terminal Fault and Meltdown V3 vulnerabilities has been added, but the other vulnerabilities still require software and microcode protection. Previous software and microcode protections would cause a performance hit on older CPUs. With the release of these new CPUs, they are powerful enough that any performance hit caused by these protections should be insignificant.

“Five Eyes” Statement on Access to Evidence and Encryption

Source: www.cnet.com

"Currently there are some challenges arising from the increasing use and sophistication of encryption technology in relation to which further assistance is needed."

Government representatives from the US, UK, Canada, Australia and New Zealand -- the so-called "Five Eyes" intelligence community -- met in Australia and discussed the future of cybersecurity, national security and the growing threat of terrorism in digital spaces. The Five Country Ministerial meeting (FCM) issued a number of joint statements, including a Statement of Principles on Access to Evidence and Encryption which came with a strong message: "privacy is not absolute." The Statement reiterated governments and tech companies have a ‘mutual responsibility’ to ensure access to ‘lawfully obtained data.’ "Providers of information and communications technology and services -- carriers, device manufacturers or over-the-top service providers -- are subject to the law, which can include requirements to assist authorities to lawfully access data, including the content of communications," the statement read. "Currently there are some challenges arising from the increasing use and sophistication of encryption technology in relation to which further assistance is needed" another statement read.

UK Proposing New Regulatory Framework for Contents Online

Source: www.buzzfeed.com

The Home Office and the Department for Digital, Culture, Media and Sport (DCMS) of the UK Government will be proposing a new regulatory framework this winter which will hold tech firms liable for contents published on their platform. This framework will give power to the Government to curb online 'social harms'. Under this the firms would be obliged to remove illegal materials or hate speech posted online within a timeframe. Failing so, they will be heavily penalised. It can also impose sanctions on social media platforms which fail to remove terrorist content, child abuse images and can also block pornography sites which don't use age verification. The firms also need to assist the police in investigating criminal activity online. There may also be the implementation of age verification for users of Facebook, Twitter and Instagram.

Kirill Kudryavtsev / AFP / Getty Images

The firms would be obliged to remove illegal materials or hate speech posted online within a timeframe.

NIST Introducing New Method of Scoring Vulnerabilities Using AI

Source: www.scmagazine.com

The U.S. National institute of Standards and Technology (NIST) will be introducing a new method of scoring publicly disclosed vulnerabilities using IBM's Watson artificial intelligence system from October 2019. IBM Watson will replace the current Common Vulnerability Scoring System (CVVS). IBM Watson will ease NIST analysts' tasks of reviewing thousands of vulnerabilities every week. IBM Watson will also produce a confidence percentage of the score calculated for each of vulnerability. It will act as a fail-safe mechanism where if the percentage falls below for 90, analysts' can take over to assess the risk score of that vulnerability. This is due to Watson's struggle for assessing the cases that are unique or highly complex like Spectre etc.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

IBM Watson will ease NIST analysts' tasks of reviewing thousands of vulnerabilities every week.

West Virginia Tested Blockchain Protected Voting in Election

Source: https://gcn.com

West Virginia became the first state in United States of America to test blockchain-protected voting in a general election. A blockchain-based mobile voting app from Voatz was used by military personnel and overseas voters to cast their votes. According to Mac Warner, West Virginia Secretary of State, it is estimated that 144 voters in 30 different countries casted their votes.

https://medium.com

Using this app, military and overseas voters qualified under the Uniformed and Overseas Citizens Act can verify their identities by providing a photo of their driver's license, state ID or passport and it is matched against their selfies. After confirmation of voters' identities, one would receive a mobile ballot like they receive in their local precinct. It uses distributed ledger technology by which one ensures that their votes cannot be tampered with after recording.

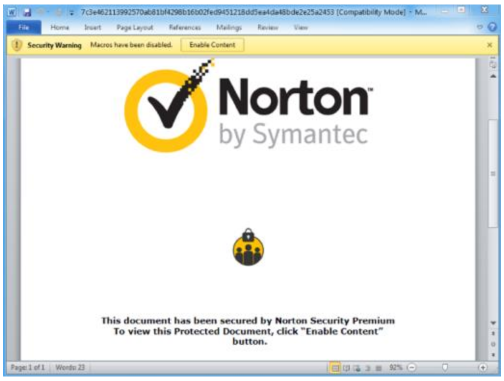
It uses distributed ledger technology by which one ensures that their votes cannot be tampered with after recording.

Malware Bytes

TA505 Responsible for Email Spam spreading the tRAT Malware

Sh. Aniruddha Kumar, NCIIPC

Threat actor TA505 is responsible for the latest email spam campaign that is spreading the tRAT malware. The malware spreads via several email campaigns. Some of these emails appear to come from well-known companies such as Norton or TripAdvisor. Others pretend to be invoices, receipts, messages or even reports from other companies. All of the email attachments are either a Microsoft Word or Microsoft Publisher file. tRat is a modular RAT written in Delphi and has appeared in campaigns in September-October 2018. Infected machine from this malware is enrolled into a specific bot. It is possible that each email campaign is creating its own botnet. Alternatively, botnets could be country, machine or operating system specific. TA505 can send new modules down to the infected machines. This allows TA505 to sell access to different blocks of machines to launch different attacks. To mitigate the risk of tRAT malware users should type URLs into their browsers themselves, instead of clicking on available links. Furthermore, users should make sure that their computer and other mobile devices are protected with up-to-date anti-virus programs, and that they are using an up-to-date version of their operating system. Users need to be aware of the risks and not open attachments in emails that they are not expecting.



This document has been secured by Norton Security Premium
To view this Protected Document, click "Enable Content" button.

Lure document from campaign on September 27, 2018, using stolen branding and social engineering to trick recipients into enabling malicious macros, *proofpoint*

To mitigate the risk of tRAT malware users should type URLs into their browsers themselves, instead of clicking on available links.

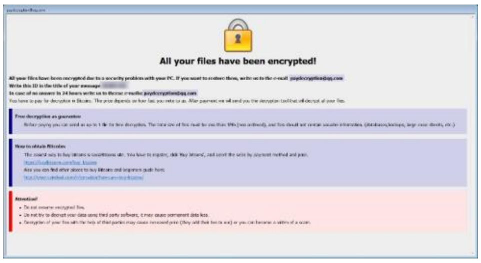
References:

[1] https://www.proofpoint.com/us/threat-insight/post/trat-new-modular-rat-appears-multiple-email-campaigns

Dharma Ransomware Installed by Remote Desktop Service

Sh. Aniruddha Kumar, NCIIPC

Dharma is a new variant of Crysis ransomware. This ransomware is manually installed by attackers who hack into Remote Desktop Services connected directly to the Internet.



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail paydecryption@qq.com
Write this ID in the title of your message [redacted]
In case of no answer in 24 hours write us to theese e-mails: paydecryption@qq.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

These attackers will scan the Internet for computers running RDP, usually on TCP port 3389, and then attempt to brute force the password for the computer. After successful infiltration, it encrypts stored file using asymmetric cryptography. When encrypting a file, it will append an extension in the format of .id-[id].[email].xxx. For example, a file called test.txt would be encrypted and renamed to test.txt.id-AC197B68.[recoverdata@protonmail.com].combo. After encrypting the files, the ransomware pops up two different ransom notes on the victim's computer. One is the Info.hta file, which is launched by an autorun when a user logs into the computer. The other note is called FILES ENCRYPTED.txt and can be found on the desktop. These files can be unlocked only through a Bitcoin payment. To protect your computer from file encryption ransomware restore your computer to a previous date, download and scan your PC with malware removal software to eliminate any remaining Dharma ransomware files.

These attackers will scan the Internet for computers running RDP, usually on TCP port 3389, and then attempt to brute force the password for the computer.

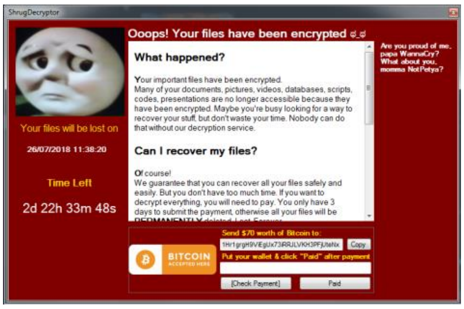
References:

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

A New .NET Framework Built Shrug Ransomware

Source: https://blogs.quickheal.com

Quick Heal Security Labs observed a new .NET framework-built Shrug ransomware. Shrug uses a random key generation for each user but due to mistakes in code, author left the keys needed to unlock the files in the directory, unintentionally enabling victims to retrieve their files without paying the ransom. The keys were found embedded in the registry, completely unencrypted. In order to decrypt ransomware, victim needs to restart the machine to terminate the process that the ransomware uses to lock the mouse and keyboard. Following that, they need to open File Explorer and enter the Shrug ransomware installer path: C:\Users\USERNAME\AppData\Local\Temp\shrug.exe. From there, users can perform a permanent delete of the shrug.exe installer file. Next, enter 'Regedit' in order to get to the registry HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run. Users can identify the key value titled 'Shrug', which can be deleted. Finally, they need to clear it from the recycle bin, restart the machine, and then the ransomware is removed.



Ooops! Your files have been encrypted ಠ_ಠ

What happened?

Your important files have been encrypted.
Many of your documents, pictures, videos, databases, scripts, codes, presentations are no longer accessible because they have been encrypted. Maybe you're busy looking for a way to recover your stuff, but don't waste your time. Nobody can do that without our decryption service.

Can I recover my files?

Of course!
We guarantee that you can recover all your files safely and easily. But you don't have too much time. If you want to decrypt everything, you will need to pay. You only have 3 days to submit the payment, otherwise all your files will be PERMANENTLY deleted. Lost Forever.

Are you proud of me, papa WannaCry? What about you, momma NotPetya?

Your files will be lost on

26/07/2018 11:38:20

Time Left

2d 22h 33m 48s

Send $70 worth of Bitcoin to:

1Hr1grgH9VEgUx73iRRJLVKH3PFjUteNx

Put your wallet & click "Paid" after payment

Ransom Note

Shrug uses a random key generation for each user but due to mistakes in the attack's code, author left the keys needed to unlock the files in the directory

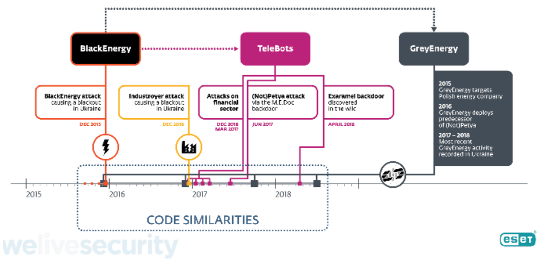
Ukraine Detected Backdoor Targeting Former Soviet States

Source: https://arstechnica.com

The Computer Emergency Response Team of Ukraine and the Foreign Intelligence Service of Ukraine detected a new strain of the Pterodo Windows backdoor targeting computers at Ukrainian government agencies.

The latest version activates only on Windows systems with language localization for Ukrainian, Belarusian, Russian, Armenian, Azerbaijani, Uzbek, Tatar, and others associated with former Soviet states.

Pterodo is a custom backdoor used to insert other malware and collect information. The new version of this malware generates a unique URL for command and control based on the serial number of the hard drive of the infected system. Data about the infected system is uploaded to that URL, allowing the attackers to analyse which tools to remotely install and run. The domains associated with the attack so far include updates-spreadwork.pw, dataoffice.zapto.org, and bitsadmin.ddns.net. This malware is used for cyber espionage operations. The latest version activates only on Windows systems with language localization for Ukrainian, Belarusian, Russian, Armenian, Azerbaijani, Uzbek, Tatar, and others associated with former Soviet states.


BlackEnergy
TeleBots
GreyEnergy
BlackEnergy attack causing a blackout in Ukraine
DEC 2015
Industroyer attack causing a blackout in Ukraine
DEC 2016
Attacks on financial sector
DEC 2016 MAR 2017
(Not)Petya attack via the M.E.Doc backdoor
JUN 2017
Exaramel backdoor discovered in the wild
APRIL 2018
2015 GreyEnergy targets Polish energy company
2016 GreyEnergy deploys predecessor of (Not)Petya
2017 – 2018 Most recent GreyEnergy activity recorded in Ukraine
2015
2016
2017
2018
CODE SIMILARITIES
welivesecurity
eset

It can be considered as the successor of the BlackEnergy toolkit because of the similar malware design, specific choice of targeted victims, and its methodology

It conducted reconnaissance and cyber espionage activities in Ukraine and Poland, focused its activities on energy and transportation industries, and other high-value targets.

GreyEnergy Targeting ICS Running SCADA Software

Source: https://www.welivesecurity.com

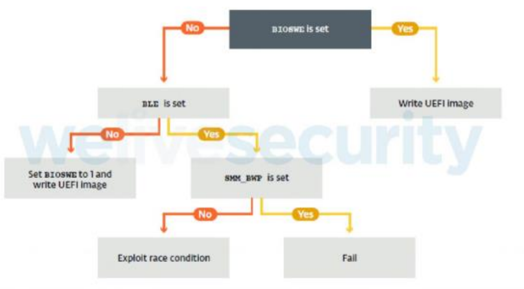
Security researchers from ESET published a detailed analysis of recently discovered cyber espionage group tracked as GreyEnergy. Its activity emerged in concurrence with BlackEnergy operations. It conducted reconnaissance and cyber espionage activities in Ukraine and Poland, focused its activities on energy and transportation industries, and other high-value targets. This malware has a modular architecture. The functionality of the malware can be easily extended with additional modules. The list of available modules includes components for file extraction, screenshot capturing, keylogging, password, credential stealing, and various kinds of backdoor. GreyEnergy operators have been strategically targeting ICS control workstations running SCADA software and servers. Attackers spread the malware by both spear phishing campaigns as well as by compromised self-hosted web services, in this latter case attackers hack into public-facing web services running on a server that is connected to an internal network. The spear-phishing messages first drop a lightweight first-stage backdoor tracked as GreyEnergy mini to gather information on the target network and gather admin credentials using tools such as Nmap and Mimikatz. The stolen credentials are used to deploy the main GreyEnergy malware into the target network with administrator privileges.

Cyberattack that Uses UEFI Rootkit

Source: https://www.welivesecurity.com

ESET researchers discovered a cyberattack that uses a Unified Extensible Firmware Interface (UEFI) rootkit named as LoJax to establish a presence on victims’ computers.

A rootkit is a dangerous malware designed to gain 'illegal' and persistent access to what is otherwise not allowed. Typically, a rootkit also masks its existence or the existence of other malware. This rootkit was part of a campaign run by the infamous Sednit group against several high-profile targets in Central and Eastern Europe, and is the first-ever publicly known attack of this kind. A UEFI rootkit is a rootkit that hides in firmware, and there are two reasons for this type of rootkit being extremely dangerous. First, UEFI rootkits are very persistent, able to survive a computer's reboot, re-installation of the operating system and even hard disk replacement. Second, they are hard to detect because the firmware is not usually inspected for code integrity. UEFI rootkits are extremely dangerous tools, used to launch cyberattacks. It is hard to detect such malware in initial stage but for remediation re-flashing the chip with a clean firmware always helps. If this is not possible, then the only remaining option is replacing the computer's motherboard. Users can protect themselves from this rootkit threat by enabling Secure Boot, use the most updated UEFI/BIOS and the most modern chipsets with the Platform Controller Hub.



This rootkit was part of a campaign run by the infamous Sednit group against several high-profile targets in Central and Eastern Europe, and is the first-ever publicly known attack of this kind.

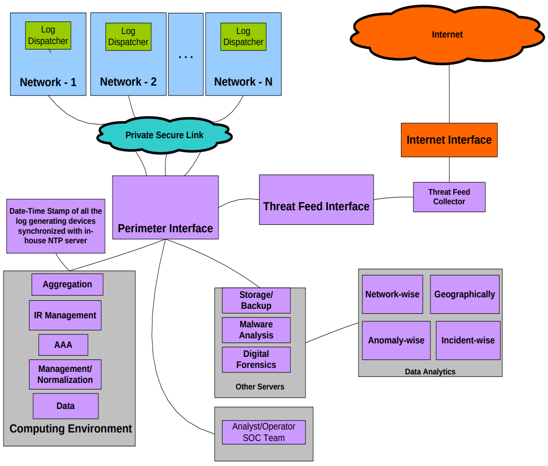
Learning

Next Generation Security Operations Centre (SOC)

Sh. Navdeep Pal Singh, NCIIPC

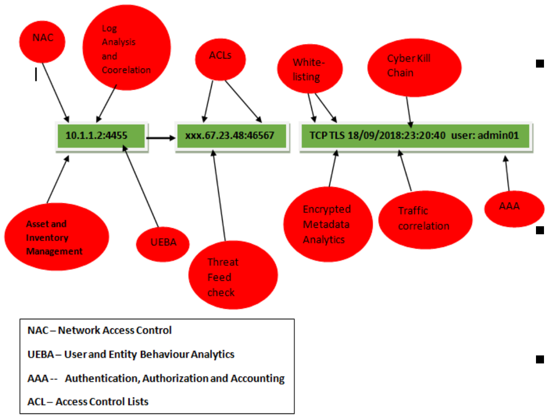
Cyber incidents are inevitable despite the layered security approach followed by Critical Information Infrastructure organisations (CIIs). Hence, it is expected that CIIs should collect, store and analyse massive amount of security events and compliance data which will support in pro-active, effective and timely incident response thereby resulting in minimal Mean Time to Recover (MTTR) and increasing Mean Time Between Failure (MTBF). At national level, similar activities are being undertaken by NCIIPC to maintain a resilient cyber space for the protection of CIIs.

Key Parameters for Next Gen SOC: The SOC should envisage for solutions which are actionable, flexible and dynamic to cater for the changing needs of Cyber Security. It must play an active role in protecting Critical Information Infrastructures in real time as indicated in adjacent diagram. Salient objectives of SOC are:



SOC must play an active role in protecting Critical Information Infrastructures in real time

- State-of-the-art Security Operation Centre will collect, monitor and analyse data/feeds for situational awareness, threat forecasting and efficient incident response in real time.


NAC
Log Analysis and Coorelation
ACLs
White-listing
Cyber Kill Chain
10.1.1.2:4455
xxx.67.23.48:46567
TCP TLS 18/09/2018:23:20:40 user: admin01
Asset and Inventory Management
UEBA
Threat Feed check
Encrypted Metadata Analytics
Traffic correlation
AAA
NAC – Network Access Control
UEBA – User and Entity Behaviour Analytics
AAA -- Authentication, Authorization and Accounting
ACL – Access Control Lists

Indicative outlook for encrypted traffic

- SOC should cater for all possible security events and artefacts from within the entire organization with pan India network and offshore presence which will enable CII to detect, identify, predict and respond to cyber kill chain and cyber threats.
- The envisaged architecture should provide high availability network with necessary security measures to exchange information securely among the different verticals of the CII across or outside the country.
- Exhaustive V/T/R (Vulnerability/Threat/Risk) assessment should be undertaken to identify and align the Critical assets in the CII to the envisaged SOC.
- Response time is another factor which highlights the amount of time taken by SOC to respond to the particular event which will also highlight the attacker dwell time (duration of the attacker in the network) in-case of intrusion.
- It should provide adequate environment with the right combination of people, process and technology to carry out necessary analysis for early detection of anomalies. Indicative outlook for encrypted traffic is highlighted in diagram adjacent.
- Automation and Report Orchestration plays the significant role in helping the SOC team to focus more on high thrust areas of pro-active analysis and incident response rather than involving in mundane tasks.
- Sound security framework needs to be embedded in the SOC as per the Critical business processes of the CII. These security frameworks highlight the security controls to be in place. NCIIPC control guidelines can also be referred for the guidance.
- SOC improvisation is must to keep abreast of the latest threats to attain the SOC maturity by deliberating on the key efficiency parameters. Indicative parameters include:
  - Time between the intrusion and detection.
  - Total time for detection to eradication of the intrusion.
  - Event handling time.
  - Number of false positives.
  - Recurrence of incidents.
  - Behavioural analytic detection.
  - Cyber Kill Chain detection.
  - Link analysis and Correlation
  - Encrypted Metadata Analytics.

It will provide adequate environment with the right combination of people, process and technology to carry out necessary analysis for early detection of anomalies.

- SOC and Network Operations Centre (NOC) are both vital function in the Network architecture. Though each has its own functions and responsibilities but small subset overlaps aim towards the continuity of the critical business process. This amalgamation of SOC and NOC will lead to accurate detection, reduced false positives and improved prevention.

This amalgamation of SOC and NOC will lead to accurate detection, reduced false positives and improved prevention.

Conclusion: Next Gen SOC should allow collating the information from different IT/OT devices in different formats to be captured, indexed, normalized and analysed, highlighting and linking the possible Indicators of Compromise (IOC) across the networks in a CII with maximum automation and report orchestration with right combination of People, Processes and Technologies.

References:

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

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

[3] https://www.nettitude.com

[4] https://www.techrepublic.com

[5] https://www.mitre.org

Cyber Security in Aviation Industry

Sh. Abhijeet Raj Shrivastava & Sh. Chandramohan, NCIIPC

Airports and the air traffic networks upon which global aviation relies are rightly considered national assets because of their importance to transport infrastructure. Allied to the fact that they also have an enormous reliance on computer networks and technology just to operate on a day-to-day basis, the infrastructure is increasingly at an elevated risk of cyber-attack. Digital technologies are used by air traffic management, airports and supply chains for efficiencies. For instance, aircraft systems connected to ground services with live monitoring allows for quicker and more cost-effective identification of service issues while airborne. One failure in the airline industry could cause terrible cascading effects, such as the mass grounding of planes and cancellation of flights.

One failure in the airline industry could cause terrible cascading effects, such as the mass grounding of planes and cancellation of flights.

Wi-Fi on aircraft is increasingly offered because it provides customers with entertainment and a method of communication in the air. Wi-Fi also allows airlines to engage with patrons and capitalize on services. However, Wi-Fi on a plane is not secure.

This means anything done on a laptop or phone using the aircraft's network could potentially be hacked. IP voice system that is used to communicate between the ground and pilots may be affected.

A particular vulnerability amongst aircraft and airline operators is the Aircraft Communications Addressing and Reporting System (ACARS), a digital air-to-ground communication network. It is an unencrypted openly transmitted messaging system that lacks security. Cyber threats that successfully penetrate ACARS could provide bogus flight plan updates, false weather information and fake messages between aircraft and ground controls. Furthermore, many aircraft have ACARS connected to the Flight Management System, which directs navigation routes, databases and airfield details. Linking these systems transmits flight plans efficiently, but they are also more exposed to risks since unauthorized parties could potentially access data. On a larger scale, baggage control systems, runway lighting and energy supply management are controlled by Supervisory Control and Data Acquisition (SCADA) systems.

A particular vulnerability amongst aircraft and airline operators is the Aircraft Communications Addressing and Reporting System (ACARS), a digital air-to-ground communication network. It is an unencrypted openly transmitted messaging system that lacks security.

Current digitalisation trends present a new challenge to airports cyber security. But airports and Operators can improve their cyber security measures in the aviation industry by working together. Foundational steps need to take to ensure that adequately protected against the threat of a cyber-attack.

- Increase their resistance to this unfamiliar threat
- Prevent access to and leakage of sensitive information
- Build the leadership and governance needed to improve cyber security
- Take practical steps to guarantee safety across all airports globally.
- Fundamentally, the focus on physical security needs to be applied with the same rigour in the cyber arena if airports are going to build resilience to potentially catastrophic cyber-attacks.
- Implement a review of organizational policies, procedures, and the current cyber security design to identify threats, vulnerabilities, and other impacts to system integrity and network communications. Both current and emerging cyber threat scenarios need to be evaluated, findings documented, and remediation recommendations provided.
- Develop the framework and processes needed to implement, monitor, and manage security operations and assets. Define standards and write best practices into your airport's governance framework to make sure cyber security isn't an afterthought in day-to-day operations.

- Design and build a complete security system that provides a layered and adaptable environment for your information technology, operational technology, networks and communications systems, including both electronic and physical security.
- Layering effective security operations protocols and support including consulting, staff augmentation, and turnkey security operations such as virus and patch management, intrusion detection and prevention, asset management, change management, incident response, and security help desk operation are all critical. Ongoing security operations are as important as setting the right policies and procedures up in the first place.
- Deploy a staff education program that baselines risky behaviours, educates employees on individual responsibility and measures performance. Insider threat - both intentional and unintended - is one of the most prevalent cyber security risks to any business and the aviation industry is no different.

Deploy a staff education program that baselines risky behaviours, educates employees on individual responsibility and measures performance. Insider threat - both intentional and unintended - is one of the most prevalent cyber security risks to any business and the aviation industry is no different.

At each stage of the process, need to proactively test controls and barriers to determine the degree to which sites, systems, and networks are vulnerable and explore mitigation steps.

References:

[1] https://www.sita.aero/air-transport-it-review/articles/lets-tackle-the-cyber-threat-in-aviation

[2] https://www.airport-technology.com/news/airports-need-beef-security-system-deal-cyber-attacks/

[3] http://www2.paconsulting.com/airport-cyber-security.html?_ga=2.183398895.897216911.1542349029-1333395154.1542349029

[4] https://www.realcleardefense.com/articles/2018/03/19/cyber_threats_to_the_aviation_industry_113216.html

Vulnerabilities in Drones

Sh. Ankit Sarkar, NCIIPC

Drones communicate wirelessly with ground pilot. Communication with payload, like a camera or sensor also occurs. Frequency spectrum depends on type of drone, flight characteristics, and payload. Drones are becoming smaller, lighter, efficient, and cheaper. Hence, future applications and deployment of drones is highly probable. Drones are remote controlled aircrafts with operating system. The absence of a pilot necessitates certain level of autonomy to deal with variable situations using pre-programmed rulesets.

Modern drones have dual Global Navigational Satellite Systems (GNSS) such as GPS and GLONASS. Flight controllers and main boards with programmable code can be hacked. Most UAVs use Linux while some use Windows. The Linux Foundation launched an open source, collaborative Dronecode project in 2014, to bring together existing and future open source UAV projects under non-profit structure. It results in common, shared open source platform for UAV. Many Drones are plagued by vulnerabilities giving root access to attackers, enabling read, delete files, or crash the device. Recently, vulnerability in widely sold Chinese DJI Drones was discovered allowing an attacker access to user's DJI account. This could provide access to:

Recently, vulnerability in widely sold Chinese DJI Drones was discovered allowing an attacker access to user's DJI account.

- Flight logs, photos and videos generated during flights, if synced DJI cloud.
- Live camera and map view during flights, of a user using DJI's FlightHub flight management software.
- Profile and DJI user's account Information.

DJI uses cookie that attacker can obtain to identify user and create tokens, to access their platforms. Through the use of XSS in this cookie, attacker can hijack any user's account and take control over DJI Mobile Apps, Web Account or FlightHub account. US-CERT published a warning about DBPOWER U818A WiFi quadcopter vide CVE-2017-3209. The researcher who reported this claims that, multiple drone models manufactured by same company are also vulnerable. Also, it uses BusyBox 1.20.2, released in 2012, vulnerable due to older version. Remote user within range of open access point on drone may utilize the anonymous user of FTP server to read images and video recorded by the device, or to replace system files and gain further access. Swann Network Video Recorder (NVR) devices contain hard-coded password and do not authenticate to view the video feed through specific URLs (CVE-2015-8286 + 8287). Remote attacker with knowledge of correct URL may stream live video from IP camera connected to NVR.

A drone receives and emits different signals for flight. Wireless communication channels are not protected making drones vulnerable to hacking risks.

Mastering a flying drone and safeguarding data collected are major issues for development of drone technology. A drone receives and emits different signals for flight. Wireless communication channels are not protected making drones vulnerable to hacking risks. The reason of this security flaw is: implementing protection systems increases manufacturing costs, while reducing autonomy in flight. One of main concerns in drones engineering is optimisation of flight-time autonomy ratio (power/weight/consumption). So, the current-generation drones are sensitive to:

- Rising signals (received by drone: radio command, GPS, etc.) can be affected by fake signals.

These signals, of identical characteristics but higher power, have "recovering" effect of weakest signal. This allows attacker to displace signal of a radio command and take control of flying drone. GPS distortion is also possible.

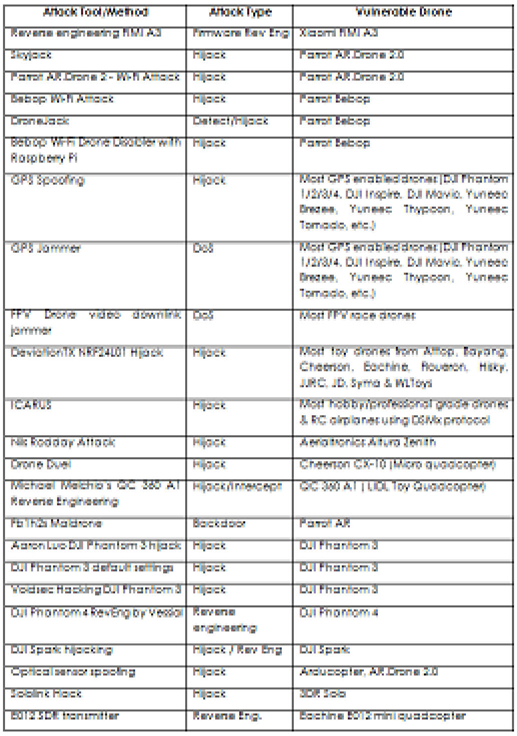
- Downlink signals (emitted by drone: video retransmission, flight information, etc.) involve risk of interception or alteration of transmitted data. Video feedback is generally transmitted on non-secured radio waves. So, each receiver correctly configured and close enough to emission point can receive data.

Video feedback is generally transmitted on non-secured radio waves. So, each receiver correctly configured and close enough to emission point can receive data.

Some drones use smartphone apps as device controller and Wi-Fi for connectivity. Such drones may be overloaded with large number of successive connection requests, requesting control of device causing CPU shut down and drone crash. Packets of data exceeding capacity allocated by buffer of drone's flight application may be sent, causing crash. A fake machine may pose as drone by constantly sending fake information packet to controller. Connection with actual drone cuts off, causing emergency landing.

Malware are designed to hack drones via Internet. Drones can also be used as zombies to hack other drones and control them. Military drone hackers try confusing drones by manipulating GPS. There are three main security issues with drones:

- Open access point
- Misconfigured FTP server
- Unwanted open ports



Attack Tool/Method	Attack Type	Vulnerable Drone
Reverse engineering RMI A3	Firmware Rev Eng	Xiaomi RMI A3
Skyjack	Hijack	Parrot AR.Drone 2.0
Parrot AR.Drone 2 - Wi-fi Attack	Hijack	Parrot AR.Drone 2.0
Bebop Wi-fi Attack	Hijack	Parrot Bebop
DroneJack	Detect/Hijack	Parrot Bebop
Bebop Wi-Fi Drone Disabler with Raspberry Pi	Hijack	Parrot Bebop
GPS Spoofing	Hijack	Most GPS enabled drones (DJI Phantom 1/2/3/4, DJI Inspire, DJI Mavic, Yuneec Breeze, Yuneec Thypoon, Yuneec Tornado, etc.)
GPS Jammer	DoS	Most GPS enabled drones (DJI Phantom 1/2/3/4, DJI Inspire, DJI Mavic, Yuneec Breeze, Yuneec Thypoon, Yuneec Tornado, etc.)
FPV Drone video downlink jammer	DoS	Most FPV race drones
DeviationTX NRF24L01 Hijack	Hijack	Most toy drones from Attop, Bayang, Cheerson, Eachine, Floureon, Hisky, JJRC, JD, Syma & WLToys
ICARUS	Hijack	Most hobby/professional grade drones & RC airplanes using DSMx protocol
Nils Rodday Attack	Hijack	Aerialtronics Altura Zenith
Drone Duel	Hijack	Cheerson CX-10 (Micro quadcopter)
Michael Melchio's QC 380 AT Reverse Engineering	Hijack/Intercept	QC 380 AT (UDI Toy Quadcopter)
FB1H2S Maldrone	Backdoor	Parrot AR
Aaron Luo DJI Phantom 3 hijack	Hijack	DJI Phantom 3
DJI Phantom 3 default settings	Hijack	DJI Phantom 3
Voidsec Hacking DJI Phantom 3	Hijack	DJI Phantom 3
DJI Phantom 4 RevEng by Vessol	Reverse engineering	DJI Phantom 4
DJI Spark hijacking	Hijack / Rev Eng	DJI Spark
Optical sensor spoofing	Hijack	Arducopter, AR.Drone 2.0
Sololink Hack	Hijack	3DR Solo
E012 SDR transmitter	Reverse Eng.	Eachine E012 mini quadcopter

There are now many kinds of Drone attack tools available

Security is not a major concern for drone manufacturers; therefore, these issues can be best handled when owner is aware and takes a wise decision according to deployment scenarios. It may help if buyer coordinates with manufacturer and optimality balancing security and operational utility are decided.

References:

[1] https://www.springer.com/cda/content/document/cda.../9789462651319-c2.pdf

[2] https://www.dummies.com/consumer-electronics/drones/understanding-how-your-drone-is-controlled/

[3] https://www.dronezon.com/learn-about-drones-quadcopters/what-is-drone-technology-or-how-does-drone-technology-work/

[4] https://research.checkpoint.com/dji-drone-vulnerability/

[5] https://threatpost.com/many-commercial-drones-insecure-by-design/125420/

[6] https://www.kb.cert.org/vuls/id/334207/
https://www.kb.cert.org/vuls/id/923388/

[7] http://www.gmconsultant.com/en/cyber-vulnerability-of-drones-a-windfall-or-a-threat/

[8] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-team-exposes-vulnerabilities-in-drones

[9] https://computer.howstuffworks.com/hack-drone.htm

Best Practices for Response and Reporting of Cyber Incidents

https://www.justice.gov/criminal-ccips/file/1096971/download

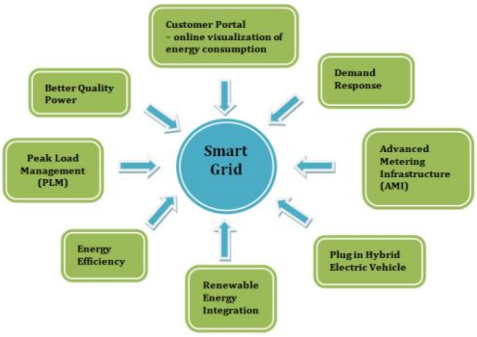
Any Internet connected organization can fall prey to a disruptive network intrusion or costly cyber-attack. A quick, effective response to a cyber incident can be critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, before a data breach incident, ransomware attack, or other cyber incident occurs. The US department of justice published the 'best practices' document to help organizations prepare a cyber incident response plan and, more generally, to better equip themselves to respond effectively and lawfully to a cyber incident. It distils lessons learned by federal investigators and prosecutors and input from private sector companies that have managed cyber incidents. It includes advice on preventing cyber incidents, as well as advice on working effectively with law enforcement. It may be useful for organizations in handling cyber incidents appropriately.

The best time to plan such a response is now, before a data breach incident, ransomware attack, or other cyber incident occurs.

Smart Grid - Security Challenges

Sh. Arun Sharma & Sh. Pradip Kumar Dixit, NCIIPC

Smart Grid is also recognised as the Advanced Metering Infrastructure (AMI). It will allow for monitoring and control of all grid activities. The AMI infrastructure expands the capabilities of the simpler and/or older system, Automated Meter Reading (AMR), which simply collects meter readings and matches them with user accounts. The data is collected locally and transmitted via Local Area Network (LAN) to a data concentrator. There are two main methods to transmit data i.e. Radio Frequency (RF) or Power Line Carrier (PLC).

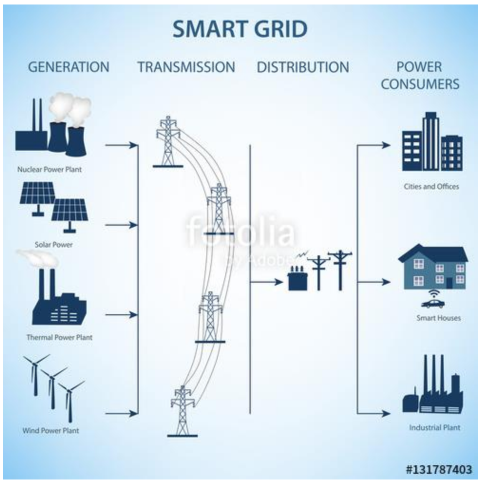

Customer Portal – online visualization of energy consumption
Demand Response
Better Quality Power
Smart Grid
Peak Load Management (PLM)
Advanced Metering Infrastructure (AMI)
Energy Efficiency
Plug in Hybrid Electric Vehicle
Renewable Energy Integration

A Smart Grid Vision – India

Major Attack Challenges on Smart Grid

Communication Network: Network that link more frequently to other networks introduces common vulnerabilities. More interconnections present will increase the chances of 'Denial of Service Attack' and introduction of Malicious Code (in Software/Firmware).

As the number of Network Nodes increase, the number of entry points and path potential adversaries might exploit will also increase. Extensive data gathering and two-way information flows may broaden the potential for compromises of data confidentiality and breaches of customer privacy.



Taxonomy of Smart Grid

Service Provider: Instead of targeting the server directly the attacker may try to infiltrate the utility network. This can be accomplished via a malicious email attachment, infected USB drive, etc. This type of attack is similar to the one used by the famous Stuxnet Malware, that was able to penetrate the air gapped network of Iranian nuclear setup. Some of the greatest risks to the successful implementation of the Smart Grid are related to the vast amounts of private data that must be transmitted and the potential for meter tampering and fraud. In particular, if a security vulnerability is found on a class of meters that leads to wide spread fraud (i.e. artificially lowering the usage or not reporting measurements) it can have devastating consequences for the utilities.

Instead of targeting the server directly the attacker may try to infiltrate the utility network. This can be accomplished via a malicious email attachment, infected USB drive, etc. This type of attack is similar to the one used by the famous Stuxnet Malware, that was able to penetrate the air gapped network of Iranian nuclear setup.

Firmware upgrade: An important attack vector is Firmware upgrades. This attack vector is of great importance and creates challenges that utilities have not yet faced. [1, 2]

Recommended Measures: In order to mitigate some of the risks, it is recommended to adopt some of the features, as following:

- First, the collection of data according to its purpose e.g., billing or by any sanitization of information whose intent is privacy.
- Second, calculations may be done directly on encrypted data to prevent its decryption or transmission in plain-text.

In a Smart Grid, the distribution level can remotely read data from the meters and send connect and disconnect commands that affect the supply of customers. It can also be viewed as a micro-SCADA Command and Control System (which is a system for local & remote control applications suitable for electrical & non-electrical processes). Therefore, a high-level architecture for privacy conscious infrastructure may be designed, which will add new functional components namely the Privacy Preserving Nodes (PPNs) to the Smart Grid. In essence, the PPNs will collect and aggregate customer data masked by homomorphic encryption (which allows computations to be carried out on cipher texts and generate an encrypted result which, when decrypted, matches the result of operations performed on the plain text) in order to protect the final User's privacy.

Overall, the Smart Grid infrastructure aims to improve reliability and efficiency of the electrical grid by lowering the cost of distribution and generation. It is essential to implement the necessary security measures and adopt industry best practices to help build attack resistant smart grid infrastructure.

References:

[1] www.indiasmartgrid.org/Cyber-Security.php

[2] Deft University of Technology: http://repository.tudelft.nl/

Vulnerability Watch

Multiple Vulnerabilities in Oracle GoldenGate

https://www.tenable.com/security/research/tra-2018-31

Oracle GoldenGate is a software product that allows replicating, filtering, and transforming data from one database to another database. Monitoring Manager Subcomponent of Oracle GoldenGate is found to have multiple vulnerabilities including a critical unauthenticated Remote Stack Buffer Overflow vulnerability (CVE-2018-2913). Versions that are affected are 12.1.2.1.0, 12.2.0.2.0 and 12.3.0.1.0. It is easily exploitable and allows unauthenticated attacker with network access via TCP to compromise Oracle GoldenGate. While the vulnerability is in Oracle GoldenGate, attacks may significantly impact additional products. For Linux and Windows platforms, the CVSS score is 9.0. For all other platforms, the CVSS score is 10.0. Oracle released patches for these vulnerabilities in the October 2018 Critical Patch Update.

It is easily exploitable and allows unauthenticated attacker with network access via TCP to compromise Oracle GoldenGate.

Critical Vulnerability in IBM API Connect

https://www-01.ibm.com/support/docview.wss?uid=ibm10728517

IBM API Connect is a comprehensive end-to-end API lifecycle solution that enables the automated creation of APIs. IBM API Connect version 2018.1.0-2018.3.4 is found to be vulnerable to Server Side Request Forgery via a proxy service (CVE-2018-1789). It has a CVSS 3.0 Base Score of 9.9. The vulnerability is addressed in IBM API Connect V2018.3.5.

The vulnerability is addressed in IBM API Connect V2018.3.5.

Critical Vulnerabilities in Circontrol CirCarLife

https://ics-cert.us-cert.gov/advisories/ICSA-18-305-03

Circontrol CirCarLife (Intelligent Charging Solutions for Electric Vehicles) all versions 4.3.1 and prior have critical vulnerabilities. Authentication to the device can be bypassed by entering the URL of a specific page (CVE-2018-17918). The PAP credentials of the device are stored in clear text in a log file that is accessible without authentication (CVE-2018-17922). These vulnerabilities have CVSS 3.0 Base Score of 9.8. Successful exploitation of these vulnerabilities could allow a remote attacker to retrieve credentials stored in clear text to bypass authentication, and access critical information.

These vulnerabilities could allow a remote attacker to retrieve credentials stored in clear text

Critical Vulnerabilities in Nuuo NVRmini2 and NVRsolo

https://ics-cert.us-cert.gov/advisories/ICSA-18-284-01

Nuuo NVRmini2 and NVRsolo (Network Video Recorders), all versions 3.8.0 and prior, are affected with critical vulnerabilities. Stack-based buffer overflow vulnerability has been identified in which there is no bounds check when a string is passed into an input buffer. As such, a remote unauthenticated attacker can overflow the stack buffer, which could allow remote code execution (CVE-2018-1149). In some cases, files exist on the file system that, when utilized, allow an unauthenticated remote attacker to gain access to and modify sensitive user information, which could allow unauthenticated remote code execution (CVE-2018-1150). NUUO has developed a fix for the reported vulnerabilities and recommends users update to firmware v3.9.1.

NUUO has developed a fix for the reported vulnerabilities and recommends users update to firmware v3.9.1

Multiple Vulnerabilities in Emerson AMS Device Manager

https://ics-cert.us-cert.gov/advisories/ICSA-18-270-01

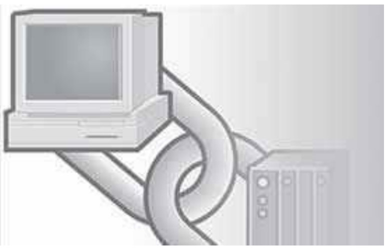
Emerson AMS Device Manager v12.0 to v13.5 is found to have multiple vulnerabilities. A specially crafted script may be run that allows arbitrary remote code execution (CVE-2018-14804). It has a CVSS 3.0 Base Score of 9.8. Non-administrative users are able to change executable and library files on the affected products (CVE-2018-14808). A CVSS v3 base score of 8.2 has been calculated. Emerson AMS Device Manager is an application for predictive diagnostics, documentation, calibration management, and device configuration for managing field instruments and digital valve controllers. Emerson recommends users patch the affected products.

A specially crafted script may be run that allows arbitrary remote code execution

Multiple Vulnerabilities in Rockwell RSLinx Classic Software

https://ics-cert.us-cert.gov/advisories/ICSA-18-263-02

RSLinx Classic, a software platform that allows Logix5000 Programmable Automation Controllers to connect to a wide variety of Rockwell Software applications, is affected with multiple vulnerabilities. Versions 4.00.01 and prior are vulnerable. This vulnerability may allow a remote threat actor to intentionally send a malformed CIP packet to Port 44818, causing the software application to stop responding and crash. This vulnerability also has the potential to exploit a buffer overflow condition, which may allow the threat actor to remotely execute arbitrary code (CVE-2018-14829). It has a CVSS 3.0 Base Score of 9.8. There are other vulnerabilities with CVE ids CVE-2018-14821 and CVE-2018-14827.

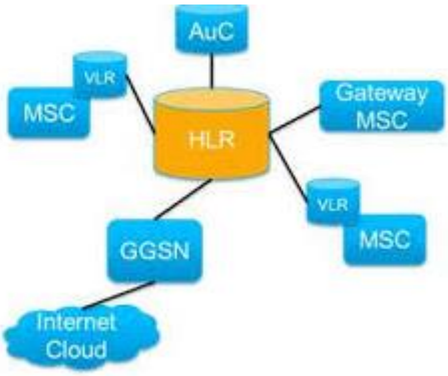


This vulnerability may allow a remote threat actor to intentionally send a malformed CIP packet to Port 44818, causing the software application to stop responding and crash.

Rockwell Automation has released a new version of the software that can be found at Rockwell Automation knowledgebase article KB 1075712.

HLR Vulnerability and Attack Exposure

Sh. Ashok Kumar Gupta, NCIIPC



A Telecom Network essentially has five elements to connect the call and transmit the data successfully. These are:

- Access Network
- Core Network
- Application and Management Network
- Internal Network and
- External Network

Cellular core networks are a vital part of Critical Information Infrastructure (CII). Core Network is responsible for service delivery and setting up end to end communication and handovers e.g. Switches, MSC, Routers, Gateways, HLR (Home Location Register) and Authentication Centre. HLR is a database from a mobile network in which information from all mobile subscribers is stored. The HLR contains information about the subscribers' identity, his telephone number, the associated services and general information about the location of the subscriber. HLR act as central repositories for all subscriber data in cellular networks. High transaction performance is essential for maintaining a usable network. HLR is known as HSS (Home Subscriber Server) in 4G network.

A successful attack on a service provider's HLR could interrupt cellular service for the entire nation.

A successful attack on a service provider's HLR could interrupt cellular service for the entire nation. Core networks are protected through separation; public access to the HLR is only possible through the cellular network, where devices have traditionally been limited in both capacity and design. Recent advances in handset technology have opened the doors to the possibility of large-scale attacks from handsets. HLR queries also create significant security and privacy issues. HLR access is also not ideally suited for next-generation network services. A typical HLR lookup can take two or three seconds to receive a response – too slow for the growing range of mobile applications for which low-latency is critical. If HLR is compromised or eavesdropped, active customer records can be stolen which might prove to be very hazardous for the National security. It can be avoided by considering removal of all necessities to hand over a subscriber's IMSI and current VLR (Visitor Location Register)/MSC to other Networks.

If HLR is compromised or eavesdropped, active customer records can be stolen which might prove to be very hazardous for the national security.

To develop a faster and more secure solution than traditional HLR access, the Telecommunication industry needs to develop a more centralised approach by building a cohesive database for number portability information, so that data can be far more easily queried by players across the mobile ecosystem. One of the benefits of a centralised approach is performance.

Unlike sluggish HLR queries, a central database generally requires less than 20 milliseconds to yield a response. This makes a centralised approach perfect for today's rising tide of VoLTE (Voice over Long Term Evolution) services and broader range of latency-sensitive applications.

References:

[1] https://searchnetworking.techtarget.com

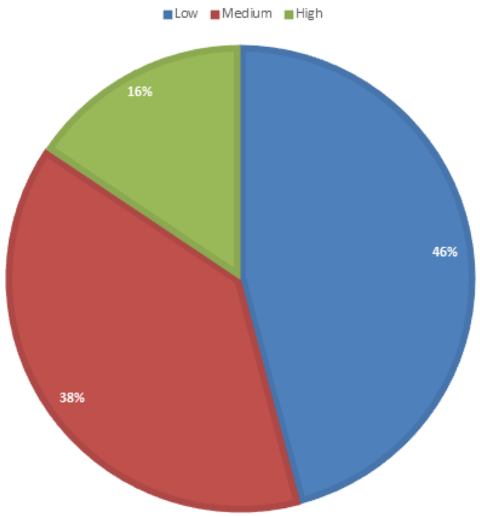
[2] https://www.techopedia.com

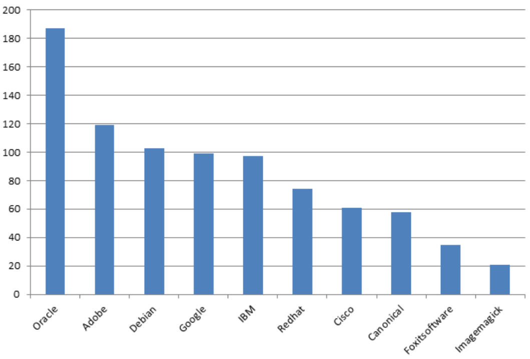
Periodic (September-November) Vulnerability Analysis

Source: *https://www.cvedetails.com*

A total of 3626 vulnerabilities have been observed during Sep-Nov 2018. Most vulnerability was reported in October with count of 1473. The low severity vulnerabilities are most with count of 1663. Maximum vulnerabilities have a score between 0-1 which is 1423 while 701 vulnerabilities have been reported with score of 4-5. During this period, maximum vulnerabilities were reported in Oracle products with a count of 187 followed by Adobe, Debian, Google and IBM.

Severity	CVSSv2 Score	Number of Vulnerabilities			Total Vulnerabilities	Total
		Sep	Oct	Nov		
Low	0-1	112	391	920	1423	1663
	1-2	3	6	0	9	
	2-3	34	26	0	60	
	3-4	73	89	9	171	
Medium	4-5	353	327	21	701	1397
	5-6	151	177	10	338	
	6-7	173	177	8	358	
High	7-8	191	178	13	382	566
	8-9	6	4	0	10	
	9-10	75	98	1	174	
Total		1171	1473	982		3626



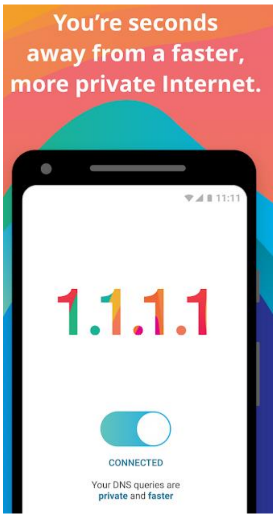


Security App

Cloudflare Promises to Speed up Internet with 1.1.1.1 Service

https://blog.cloudflare.com/1-thing-you-can-do-to-make-your-internet-safer-and-faster/

Cloudflare launched its 1.1.1.1 DNS resolver app that anyone could use free of charge. DNS services are provided by Internet Service Providers (ISP) to resolve a domain name like google.com into a real IP address for routers and switches to understand. DNS servers provided by ISPs are often slow and unreliable, and Cloudflare promises to speed up Internet with its 1.1.1.1 service. After a successful beta, it's now arriving on iOS and Android with an App named "1.1.1.1". It supports DNS-over-TLS and DNS-over-HTTPS which gives protection from Snooping DNS Queries. It will also prevent carrier from tracking browsing history and potentially selling it. Cloudflare is promising not to track 1.1.1.1 users or sell ads and to perform an annual audit and publish a public report.


You're seconds away from a faster, more private Internet.
11:11
1.1.1.1
CONNECTED
Your DNS queries are private and faster

It supports DNS-over-TLS and DNS-over-HTTPS which gives protection from Snooping DNS Queries.

Visit Firefox Monitor to see whether you were in Data Breach

https://blog.mozilla.org/blog/2018/11/14/firefox-monitor-launches-in-26-languages-and-adds-new-desktop-browser-feature

Mozilla has added a new feature in its Firefox browser which shows a notification that alerts desktop users when they visit a site that has had a recently reported data breach. "While using the Firefox Quantum browser, when you land on a site that's been breached, you'll get a notification. You can click on the alert to visit Firefox Monitor and scan your email to see whether or not you were involved in that data breach. This alert will appear at most once per site and only for data breaches reported in the previous twelve months" said Mozilla's official Blog. Apart from this, Mozilla has also made Firefox Monitor available in 26 languages to make it easier for people to learn about data breaches and take action to protect them.

You can click on the alert to visit Firefox Monitor and scan your email to see whether or not you were involved in that data breach.

Quickly Investigating Websites with Lookyloo

https://isc.sans.edu/forums/diary/Quickly+Investigating+Websites+with+Lookyloo/24320

Lookyloo is a tool developed by The Computer Incident Response Center Luxembourg (CIRCL) that helps to have a quick overview of a website by scraping it and displaying a tree of domains calling each other. The name "Lookyloo" comes from the Urban Dictionary and means "People who just come to look". The tool provides a simple web interface to submit a new site to query or to review previous analysis. For each domain, you get the following information (if detected): Presence of JavaScript, Cookie received, Cookie read, Cookie in URL.

Cloudfare's Roughtime Service

Source: http://www.eweek.com

Cloudflare announced the deployment of a new authenticated time service called Roughtime, in an effort to secure certain timekeeping efforts. Roughtime is a UDP-based protocol that benefits from cryptographic protection to help maintain integrity and limit the risk of MITM attacks. It also includes measures to help protect it from being used as an amplifier for DDoS attacks. Cloudflare intends to use its Roughtime service to help validate the proper expiration date of SSL/TLS certificates. Without the ability to properly verify time, an attacker could trick a user or server into accepting a certificate that has already expired. Cloudflare's Roughtime service is freely available at roughtime.cloudflare.com.

Cloudflare intends to use its Roughtime service to help validate the proper expiration date of SSL/TLS certificates.

Threat Hunting with OSSEC

https://isc.sans.edu/forums/diary/Hunting+for+Suspicious+Processes+with+OSSEC/24122/

OSSEC is a scalable, multi-platform, open source Host-based Intrusion Detection System. It has a powerful correlation and analysis engine, integrating log analysis; file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, MacOS, and Windows. OSSEC is a free security monitoring tool/log management platform which has features for detecting malicious activity on a live system like the rootkit detection etc.

OSSEC is a free security monitoring tool/log management platform which has features for detecting malicious activity on a live system

NCIIPC Initiatives

NSE FutureTech 2018, a Conversation about Cyber Security Threats in Today's World

https://www.nseindia.com/content/press/PR_cc_04092018.pdf

National Stock Exchange of India Ltd. (NSE), India's leading stock exchange on September 4, 2018 organized the NSE FutureTech 2018, which brought together global and local opinion makers to discuss and share technology, its ramifications and the extent to which cyber security threats are reality in today's world. It is in this context that the Capital Market eco-system is considered as one of the important segment in the National Critical Infrastructure (NCI) of any economy and rendering it vulnerable and susceptible to cyber breaches would damage and impair the economic and social fabric of the nations. Dr. Ajeet Bajpai, Director General – NCIIPC shared major NCIIPC initiatives towards Protecting Critical Information Infrastructures.

Major NCIIPC Initiatives...
Incident Response & Responsible Vulnerability Disclosure Program
Interns, Research Scholars & Cyber Security Professionals
CII Range to simulate possible real-world threat scenarios & emulate critical network components
Public Private Partnership (PPP) for Training
NSE
Future Tech 2018
Cyber Security
IN A NEW WORLD

Dr. Ajeet Bajpai, DG – NCIIPC at NSE FutureTech 2018

INFOSEC GLOBAL 2018
Cyber Resilience & Agility in Your Digital Future
Dr. Ajeet Bajpai
DG, NCIIPC(Govt. of India)
16th November, 2018
The Park, Kolkata

NCIIPC at Infosec Global 2018

'Infosec Global 2018', the 3rd International Cyber Security Summit was held in The Park, Kolkata on 16th November, 2018. "Cyber Resilience and Agility in your Digital Future" was the theme of the summit. The summit was organised by InfoSec foundation. Dr. Gulshan Rai, National Cyber Security Coordinator was the Chief Guest of the program. The summit was attended by the CISO of various national and international organisations. DG, NCIIPC delivered talk about security aspects of National Critical Information Infrastructure and its challenges.

NCIIPC at BIMSTEC Conference

IDSA-BIMSTEC (Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation) Workshop on Cyber Security Cooperation was hosted by India from 5th to 7th December 2018 at New Delhi. NCIIPC chaired the session on 'Cyber Security Preparedness and National Approaches'. It also participated in the discussions on 'BIMSTEC Cooperation in the Area of Cyber Security'. The 3-day event concluded with BIMSTEC delegates visiting NCIIPC CII Range where various aspects of cyber security challenges were demonstrated, that have potential to affect critical infrastructure elements.

NCIIPC Responsible Vulnerability Disclosure Program

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

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

- Sh. Dipak Prajapati
- Sh. Raghav Sharma
- Sh. Akash Sakhesaria
- Sh. Veerababu Penugonda
- Sh. Tarun
- Sh. Sachin Gupta
- Sh. Sumit Lakra
- Sh. Vikas
- Sh. Chirag Gupta
- Sh. Sanath
- Sh. Aagam Shah
- Sh. Aushutosh Bainsekar
- Sh. Hrishikesh Panse
- Sh. Akshay

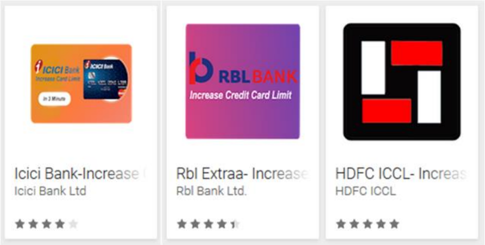
NCIIPC acknowledges the researchers for their contributions towards protection of National Critical Information Infrastructure.

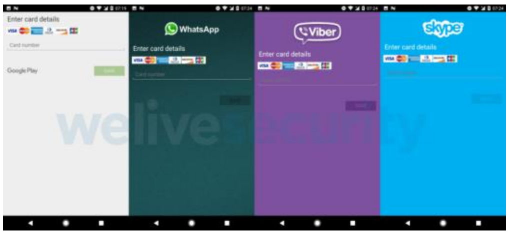
Mobile Security

Fake Android Apps in Google Playstore

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

Google Playstore is lurking with hundreds of fakes. A lot of these apps have been taken down by Google. E.g. starting from June 2018, many apps claiming to increase credit limit have been found stealing credit card details and internet banking credentials using forms which are required to be filled up within these apps. Posing as Indian banks, some of these apps furthermore leaked the stolen data online. There has also been a report of impersonation of six banks from New Zealand, Australia, The United Kingdom, Switzerland, Poland and Australian cryptocurrency exchange Bitpanda through apps. In early October 2018, 29 malicious apps were found which were remotely controlled by Trojans. An app named "Optimization Android" has also been found to compromise the users' PayPal app by malicious accessibility service and this app has also been seen to push overlay screen over users' Google Play, WhatsApp, Skype, Viber and Gmail app.


Icici Bank-Increase
Icici Bank Ltd
Rbl Extraa- Increase
Rbl Bank Ltd.
HDFC ICCL- Increas
HDFC ICCL



Facebook Bug Exposed Unposted Photos of 6.8 Million Users to Third-Party Apps

Source: https://thehackernews.com/

A programming bug in Facebook website accidentally gave 1,500 third-party apps access to the un posted Facebook photos of as many as 6.8 million users. The flaw left users private data exposed for 12 days, between September 13th and September 25th, until Facebook discovered and fixed the security blunder on the 25th September. The bug led 876 developers to access user's private photos which they never shared on their timeline, including images uploaded to Marketplace or Facebook Stories. Facebook said that when someone gives permission for an app to access their photos on Facebook, they usually only grant the app access to photos people share on their timeline. In this case, the bug potentially gave developers access to other photos, such as those shared on Marketplace or Facebook Stories.

Facebook assured its users that soon they will be rolling out tools for app developers that will allow them to determine which people using their app might be impacted by this bug. The company will be working with app developers to delete copies of photos that they were not supposed to access.

The bug led 876 developers to access user's private photos which they never shared on their timeline, including images uploaded to Marketplace or Facebook Stories.

Google Play Services Terminating Updates for Ice Cream Sandwich

Source: https://android-developers.googleblog.com/

The Android Ice Cream Sandwich (ICS API level 14 and 15) platform is Seven years old and the active device count has been below 1% for some time. This means if your phone still runs on Android Ice Cream Sandwich, Google will not be updating the Play Services APK anymore after 14.7.99. The Google Play Services SDK includes Google Play services APK interfaces to make sure certain features and functionality will work. There are apps that use Ice Cream Sandwich but that may change soon. A higher API level may still be updated or required. The Play Services APK will soon require JellyBean (API level 16).

New Keystore Features Keep your Slice of Android Pie Slightly Harmless

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

The Android Keystore provides application developers with a set of cryptographic tools that are designed to secure their users' data. Keystore moves the cryptographic primitives available in software libraries out of the Android OS and into secure hardware. Keys are protected and used only within the secure hardware to protect application secrets from various forms of attacks. Keystore gives applications the ability to specify restrictions on how and when the keys can be used.

Android Keystore provides application developers with a set of cryptographic tools that are designed to secure their users' data.

Android Pie introduces Keyguard-bound keys and Secure Key capabilities to Keystore. Keyguard binding ties the availability of keys directly to the screen lock state while authentication binding uses a constant timeout. With keyguard binding, the keys become unavailable as soon as the device is locked and are only made available again when the user unlocks the device. Hardware-enforced Android Keystore protection features like authentication binding can be combined with keyguard binding for a higher level of security. Secure Key Import is useful in scenarios where an application intends to share a secret key with an Android device, but wants to prevent the key from being intercepted or from leaving the device.

Upcoming Events - Global

January 2019

Workshop on Security issues in Cyber-Physical System, Hangzhou	3-5 Jan
s4x19 ICS Security Event, Miami Beach	14-17 Jan
SINET Global Institute CISO Series, Scottsdale	15-16 Jan
FutureCon Atlanta Cyber Security Conference, Atlanta	16 Jan
Medical Device Security 101, Orlando	20-22 Jan
Cyber Security for Critical Assets, Dubai	21-22 Jan
SANS Cyber Threat Intelligence Summit, Arlington	21-28 Jan
Cyber Defence & Network Security, London	29-31 Jan

CS4CA MENA
21st – 22nd January 2019
Dubai, UAE

JANUARY 2019						
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 2019

SANS Security East 2019, New Orleans	2-9 Feb
Annual Privacy and Security Conference, Victoria	6-8 Feb
Manusec: Cyber Security for Critical Manufacturing Europe, Munich	7-8 Feb
Cyber Security Summit, Atlanta	13 Feb
HackCon, Oslo	13-14 Feb
IoT in Oil & Gas, Calgary	13-14 Feb
Offensive Security Conference, Berlin	15-16 Feb

FEBRUARY 2019						
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		

March 2019

RSA Conference USA, San Francisco	4-8 Mar
InfoSecurity Connect, San Diego	11-13 Mar
International Workshop on Security, Privacy and Trust in the Internet of Things, Kyoto	11-15 Mar
FIRST Cyber Threat Intelligence Symposium, London	18-20 Mar
ICS Security Summit & Training 2019, Orlando	18-23 Mar
Smart Grid Cyber Security Conference, London	20-21 Mar
Cyber Security for Critical Assets USA, Houston	26-27 Mar
Symposium on Securing the IoT, San Francisco	27-29 Mar

RSAConference2019
Moscone Center | San Francisco
March 4 – 8, 2019

April 2019

SANS 2019, Orlando	1-8 Apr
Cyber Security Summit, Denver	4 Apr
Kaspersky Security Analyst Summit, Singapore	8-11 Apr

Upcoming Events - India

SANS Bangalore 2019	7-19 Jan
International Conference on Networks and Communications, Chennai	19-20 Jan
International Conference on Identity, Security and Behavior Analysis, Hyderabad	22-24 Jan
Cyber Security for Industry 4.0, Mumbai	29 Jan
3rd Internet of Things India Expo, New Delhi	29-31 Jan
IoTshow.in, Bengaluru	26-28 Feb
OWASP Seasides 2019, Goa	27-28 Feb
NULLCON, Goa	1-2 Mar
International Conference on Machine Learning, Image Processing, Networks and Data Sciences, Kurukshetra	3-4 Mar
SANS Secure India 2019, Bangalore	4-9 Mar
Gartner Application Architecture, Development and Integration Summit 2019, Mumbai	11 Mar
Gartner IT Infrastructure, Operations & Cloud Strategies Conference 2019, Mumbai	6 May

MARCH 2019

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 2019

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				

General Help		helpdesk1@nciipc.gov.in helpdesk2@nciipc.gov.in
Incident Reporting	:	ir@nciipc.gov.in
Vulnerability Disclosure	:	rvdp@nciipc.gov.in
Malware Upload	:	mal.repository@nciipc.gov.in

Notes

Feedback/Contribution

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

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