NEWSLETTER

July 2020

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

"The crisis the world is facing today teaches us that way forward is - Aatmanirbhar Bharat (A self - reliant India)"

The Mantra is to Make in India for India and the World.

Digital India
Power To Empower

Aatmanirbhar Bharat

App Innovation Challenge

"A generous heart, kind speech, and a life of service and compassion are the things which renew humanity."

"I am proud to belong to a nation which has sheltered the persecuted and the refugees of all religions and all nations of the earth."

"The golden way is to be friends with the world and to regard the whole human family as one."

India having rich heritage of World Peace and Brotherhood has the potential to fulfill the World demand for a trusted Supply Chain Partner.

https://innovate.mygov.in/

VOLUME 4 ISSUE 3

@NCIIPC

NCIIPC Newsletter

July 2020

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

The outbreak of the Covid-19 and the global efforts directed towards tackling the health epidemic have provided an opportunity to the threat actors and cyber criminals to take advantage of the imposed online activities and behavioural compulsions. NCIIPC has detected a surge in cyber-attacks due to spams, phishing campaigns, phishing domains and malicious Mobile Apps in the last three months.

While unsuspecting users may be seeking information, alerts and advisories concerning the ongoing pandemic, unscrupulous marketers, cyber criminals and threat actors have been virtually stalking the cyberspace and taking advantage of the widespread global communications on the Coronavirus to mask their activities.

Malware, Spyware and Trojans have been found embedded in interactive Coronavirus Maps and Websites. Attackers are taking advantage of the increased popularity of online collaboration platforms to distribute installers containing malware and adware. Spam E-mails are also tricking users into clicking on links which download Malware on their computers or Mobile devices.

Over 1,00,000 new domains containing terms related to Corona/COVID have been registered, of which a large percentage are suspected to be malicious. Threat actors have taken to naming attachments disguised as updates and recommendations connected to the coronavirus to entice users into clicking them thereby infecting their machines with malware. Almost 45% of the campaigns orchestrated by Advanced Persistent Threat (APT) Groups are found to be using contemporary techniques with corona themed lures.

Government of India has launched the 'Aatmanirbhar Bharat App Innovation Challenge'. This seeks to create an ecosystem where Indian entrepreneurs and Start-ups are incentivised to ideate, incubate, build, nurture and sustain technology solutions that can serve not only citizens within India but also the world.

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.

Stay Corona Safe and Cyber Secure!

News Snippets - National

Spurt in Cyberattacks on Home Networks and Routers

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

There has been a sharp in the number of cyberattacks on personal computer networks and routers since professionals were asked to work from home in the wake of COVID-19 outbreak. Cyber criminals are exploiting the COVID-19 outbreak as an opportunity to send phishing emails claiming to have important updates or encouraging donations, impersonating trustworthy organisations. Enterprise VPN servers have now become paramount to a company's backbone, and their security and availability must be the focus for IT (Information Technology) teams. It is important that VPN services are patched and kept up to date. Default passwords of home Wi-Fi router should be changed and strengthened. When employees bring work devices home, those devices should not be used by anyone else in the home. 'Remember password' functions should always be turned off when employees are logging into company information systems and applications from their personal devices.

When employees bring work devices home, those devices should not be used by anyone else in the home.

Influences on Social Media Promoting Violent Extremist Ideologies Is the Biggest Cyber Threat

Source: https://www.medianama.com, https://in.news.com

"Influences on social media" that promote "violent extremist ideologies" are among the biggest cyber threats right now, said Sh. Satish Chandra Jha, Chairman, National Technical Research Organisation (NTRO), at Nullcon conference on March 5. The other threats he mentioned were data breaches, business espionage, phishing and distributed denial of service attacks, polymorphic malware that change features to be better at contamination and supply chain contamination. He also said that India is among the top targets of global cyberattacks. During his welcome address at Nullcon Conference 2020, he also drew attention to NCIIPC's Responsible Vulnerability Disclosure Program (RVDP) that allows people to report vulnerabilities in Indian Critical information Infrastructure. Issue like lack of coordination and global policy on dealing with cyber threats was also pointed out by him.

"Lack of coordination and global policy on dealing with cyber threats at international level is a major problem": Chairman, NTRO.

PNB Housing Finance Awarded ISO 27001:2013 Standard

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

PNB Housing Finance Limited, has been awarded ISO 27001:2013 standard. It is an international standard that provides the specification for an Information Security Management System (ISMS). PNB Housing enables business workflows while ensuring

PNB Housing enables business workflows while ensuring security & controls to prevent unsolicited transactions and perpetrators of fraud.

security & controls to prevent unsolicited transactions and perpetrators of fraud. Information and alerts from all the controlling units including perimeter security, endpoint security, network security, application security, web security, email security, physical infrastructure security and identity management converge to a central unified solution giving the cockpit view of all the security vectors. This prepares PNB Housing in effectively identifying, analysing and combating cyber-attacks." At PNB Housing, all operational activities are done in a secured manner. Safeguarding customer data is paramount for us and we take a risk-based approach to information security thereby proactively identifying any threats to customers and organisations and take appropriate controls to arrest them in the early stages itself", said Nitant Desai, Chief Centralised Operation and Technology Officer, PNB Housing.

The International police organisation has red flagged a ransomware which is being spread using email camouflaged as information or advice regarding coronavirus or COVID-19 from a government agency

Criminals Targeting Hospitals and Banking Apps by Exploiting COVID Pandemic

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

The CBI has alerted all the state police about cyber criminals increasingly targeting hospitals and other vital health installations who are tackling the coronavirus pandemic. INTERPOL, the international police organisation has red flagged a ransomware which is being spread using email camouflaged as information or advice regarding coronavirus or COVID-19 from a government agency, luring the recipient to click the infected attachments. Once the attachment is opened, it blocks the recipient's access to the system till a ransom is paid, they said. Based on inputs received from INTERPOL, CBI has also issued another alert related to a banking Trojan known as Cerberus. The malicious software takes advantage of COVID-19 pandemic to impersonate and send SMS using the lure of COVID-19 related content, to download the embedded malicious link, which deploys its malicious app. This Trojan primarily focuses on stealing financial data such as credit card numbers and can capture two-factor authentication details.

Fake AarogyaSetu App to Snoop on Indian Officials

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

ISI-sponsored Pakistani hackers have created a fake AarogyaSetu app and their links were sent into the accounts of several government and army officials. The development was noticed by Maharashtra cyber intelligence and analytical cell that alerted other security agencies across the country about the threat. The malware has a look completely similar to original app. Once one downloads this fake app, the entire data of

user's mobile phone is transferred to the online crooks across the border. The fake app sends all the data to its creators. It also activates the microphone of the victim's mobile phone, and the conversations could be intercepted by the app creator.

News Snippets - International

WHO Targeted in Espionage Attempt

Source: https://threatpost.com/

DarkHotel APT group has tried to infiltrate World Health Organisation (WHO) networks to steal information. Alexander Urbelis, cybersecurity researcher at Blackstone Law Group, told Reuters that he personally observed a malicious site being set up on March 13 that mimicked the WHO's internal email system. Its purpose was to steal passwords from multiple agency staffers. CrowdStrike shared analysis with Threatpost about a scam impersonating WHO that requested Bitcoin donations to the COVID-19 Solidarity Response Fund—the name of a legitimate fund created by the WHO. The body of one message appears to be copied directly from the official website of the fund. Additionally, the scam emails spoofed WHO email addresses (e.g., using <donate@who.int>) but were not sent from valid WHO domains.

The scam emails spoofed WHO email addresses (e.g., using <donate@who.int>) but were not sent from valid WHO domains

Cloud Providers, CDNs Team up Against Internet Routing Attacks

Source: https://threatpost.com/

A group of tech giants including Akamai, Cloudflare, Google, Facebook, Microsoft, Amazon Web Services and Netflix, are joining to combat route leaks, route hijacking, and IP address-spoofing attacks targeting Internet users. They all are coming together under a program introduced by the Mutually Agreed Norms for Routing Security (MANRS) global initiative. While cloud and CDN are basically edge networks, their impact on routing security can be significant. Some known incidents showed that even a small edge network can cause havoc on the Internet by leaking routes. This new program asks cloud providers and CDN members to take these five security steps:

- Prevent the propagation of incorrect routing information
- Prevent the traffic of illegitimate source IP addresses
- Facilitate the global operational communication and

A group of tech giants are coming together under a program introduced by the Mutually Agreed Norms for Routing Security (MANRS) global initiative

coordination
- Facilitate the validation of routing information on a global scale
- Encouraging the adoption of "good practices on routing security"

"The security of our government and professional communications, as well as of our most private data, depends on our use of trusted partners from nations that share our values and our aspirations for humanity,"

US Agencies Recommend to Ban China Telecom over Cybersecurity Risks

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

Several U.S. Executive Branch agencies including the Departments of Justice, Homeland Security, Defense, State, Commerce, and the United States Trade Representative are asking the Federal Communications Commission (FCC) to block China Telecom Americas authorization to operate within the United States over significant cybersecurity risks. "The security of our government and professional communications, as well as of our most private data, depends on our use of trusted partners from nations that share our values and our aspirations for humanity," Assistant Attorney General for National Security John C. Demers said. The US agencies said that "China Telecom's U.S. Operations provide opportunities for Chinese state-sponsored actors to engage in espionage, to steal trade secrets and other confidential business information, and to disrupt and misroute U.S. communications traffic, according to the FCC filing. Following are the reasons behind the recommendation of the federal agencies to block China Telecom's operations within the U.S:

- The evolving national security environment since 2007 and increased knowledge of the PRC's role in malicious cyber activity targeting the U.S.
- China's Telecom is vulnerable to exploitation, influence, and control by the PRC government
- Inaccurate statements by China Telecom were given to U.S. government authorities about China Telecom stored its U.S. records
- Inaccurate public representations by China Telecom concerning its cybersecurity practices
- The nature of China Telecom's U.S. operations provides opportunities for PRC state-actors to engage in malicious cyber activity

ASD and NSA Issues Guidance for Combating Web Shell Malware

Source: https://www.darkreading.com/

The Web shell malware is a growing cybersecurity problem, which executes arbitrary instructions on a targeted web server.

The Australian Signals Directorate (ASD) and US National Security Agency (NSA) joined forces to issue a Cybersecurity Information Sheet on how to detect and mitigate this form of malware. This sheet includes information on how to detect Web shells, such as tips on using known-good comparison, in which a file on the Web server is compared to a "known good" version of the file stored elsewhere. The ASD and NSA also provide instructions on mitigating the threat by the use of Web flow detection, IDS/IPS technology, and file-integrity monitoring to quickly detect files which have been modified without administrator permission.

This sheet includes information on how to detect Web shells, such as tips on using known-good comparison, in which a file on the Web server is compared to a "known good" version of the file stored elsewhere.

US, UK Authorities Crack Down Suspicious COVID-19 Domains

Source: https://www.bankinfosecurity.in/

US and UK law enforcement officials have shut down suspicious domains with COVID-19 themes and names. The Justice Department reported that the suspicious domains were used for an array of scams, including spoofing the websites of legitimate companies and services, tricking victims into giving their personally identifiable information, including bank details, by inputting this data into sites that spoof government programs and agencies, stealing money by falsely claiming to collect donations to the American Red Cross for COVID-19 relief efforts. Britain's National Cyber Security Center noted that authorities have closed down nearly 470 online shops selling fake corona virus-related items as well as another 555 sites were found to be distributing malware.

Image Source: unit42.paloaltonetworks.com

Europe's Largest Private Hospital Operator Hit by Ransomware

Source: https://krebsonsecurity.com/

Fresenius, Europe's largest private hospital operator has been hit by a ransomware cyber-attack on its technology systems. The ransomware used, Snake ransomware. It is a relatively new strain that is being used to shake down large businesses, holding their IT systems and data hostage in exchange for payment in a digital currency. The INTERPOL also warned that it has detected a significant increase in the number of attempted ransomware attacks against key organizations and infrastructure engaged in the COVID-19 response. Security researchers say that Snake ransomware is somewhat unique in that it seeks to identify IT processes tied to enterprise management tools and large-scale industrial control systems (ICS), such as production and manufacturing networks.

Dark Web Ad of 47.5 Million Indians Truecaller Records for Sales

Source: https://gbhackers.com/truecaller-data-breach/

It's not hard for bad actors to compile multiple phone number databases and put a Truecaller stamp on it.

Recently it has been observed that an unprotected Amazon S3 bucket contains data from major websites. An anonymous individual was found selling on the dark web, 47.5 Million users' personal data that is associated with caller ID app Truecaller. The information was quite well organized by state, cities, and carrier. An advertisement on the dark web states that Truecaller records of 47.5 Million Indians are up for sale for $1000 only. The data found to be from 2019, and includes interesting information such as Phone Number, Carrier, Name, Gender, City, Email, Facebook ID, and others. Threat actors may use these personal details to launch sophisticated attacks targeting individuals. It's not hard for bad actors to compile multiple phone number databases and put a Truecaller stamp on it. It lends some credibility to the data and makes it easier for them to sell.

Trends

Hackers Exfiltrate Data from Air-Gapped Computers

Source: https://www.securityweek.com

To implement such an attack, attackers need to first compromise both air-gapped computer (Transmitter) and a mobile phone (Receiver) of an employee.

It is now possible for hackers to steal sensitive data from air gapped systems even when it is highly secured, by tapping into the vibrations from machine's internal fan. Previously researchers mentioned that it was possible to exfiltrate data via router LEDs, HDD LEDs, power lines, magnetic fields, heat emissions, scanners, USB Devices and screen brightness. The malware can encode binary information and modulate it over a low frequency vibrational carrier. A malicious application on a smartphone placed on the same surface, can sense and decode the generated vibrations. Malicious application can access a mobile device's sensors such as the accelerometer without asking user's permission. To implement such an attack, attackers need to first compromise both air-gapped computer (Transmitter) and a mobile phone (Receiver) of an employee. Once successfully compromised, malware on the transmitter gathers sensitive information, encodes it and sends it to the receiver via vibration on the surface.

CISA Launches Telework Product Line

Source: https://www.hstoday.us

These new products are available on cisa.gov/telework

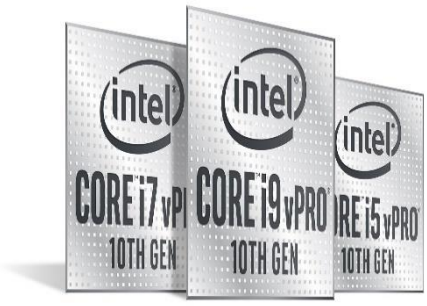
The Cybersecurity and Infrastructure Security Agency (CISA) has launched a dedicated telework product line intended to advise and support the incorporation of cybersecurity

considerations when adopting or expanding telework policies, such as the use of video conferencing software and related collaboration tools. These new products are available on cisa.gov/telework. This webpage is a one-stop shop for telework cybersecurity guidance for government, critical infrastructure and citizens. This guidance has been developed in close collaboration with federal and private sector partners. CISA provides information and advice about threat vectors, cybersecurity best practices and how to properly apply security settings for a range of video conferencing tools.

Intel Improves Hardware Shield in 10th Gen Core vPro Processors

Source: https://www.securityweek.com

Intel has announced its new 10th Gen Core vPro processors which include an enhanced version of Hardware Shield that provides advanced threat detection capabilities. It is also designed to provide better performance, built-in security features, and fast and reliable connectivity with integrated Wi-Fi 6. Security in BIOS and Firmware level has been taken care by company. Intel Hardware Shield now appends advanced threat detection and extended protection beyond system memory to help improve the detection of advanced threats while reducing false positives and reducing performance impact. Hardware Shield "helps ensure the OS runs on legitimate hardware and provides hardware-to-OS security reporting to enable OS to enforce a more comprehensive security policy. The vPro platform also adds Transparent Supply Chain which provides a mechanism for confirming that a component is authentic.

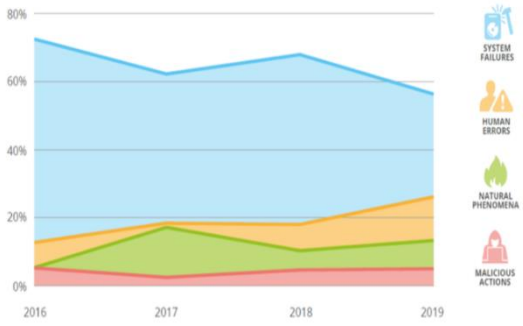


Designed to provide better performance, built-in security features, and fast and reliable connectivity with integrated Wi-Fi 6.

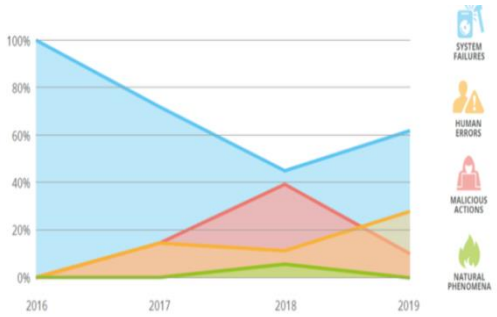
Spotlight: Incident Reporting of Telecom Security

Telecom Sector, NCIIPC

ENISA, the EU Agency for Cybersecurity, released a new version of Cyber Incident Reporting and Analysis System (CIRAS), a tool for statistical analysis of cybersecurity incidents. The online visual tool, accessible to the public, gives access to 8 years of telecom security incidents, and 4 years of trust services incident reports i.e. total of 1100 cybersecurity incidents. Cybersecurity incident reporting gives the national authorities in Europe vital information about the root causes and overall impact of major incidents. Every year national authorities send summaries of these major cybersecurity incidents to ENISA for aggregation and analysis at EU level. ENISA publishes statistics in yearly



Root cause of telecom security incidents



Root cause categories of trust services security incidents

reports and gives access to aggregated and anonymised data in the online visual tool, to increase transparency about cybersecurity incidents. This online visual tool allows for custom analysis of trends and patterns. For example, the user is able to select a specific time-period or specific root cause category and get custom statistics about detailed causes and assets affected. ENISA also maintains a private repository for the national authorities.

Root causes of telecom security incidents: Over the last 4 years, the most common root cause of telecom security incidents is system failure (412 out of 637 incidents). The second most common root cause is human error, with nearly a fifth of total incidents (19%, 119 incidents in total). Natural phenomena are the third root cause with 11%, while only 4% of the incidents are categorized as malicious actions.

Root cause categories of trust services security incidents: Over the 4 years of trust services security incident reporting, the most common root cause is System failure (60%). Around a fifth of the reported incidents were due to human errors and a fifth of the incidents were flagged as malicious actions. Natural phenomena are not a common root cause in this sector. This sector operates differently than the telecom one. With large-scale above ground infrastructure for the mobile networks, the telecom sector is more vulnerable to natural phenomena.

References:

[1] https://www.enisa.europa.eu/news/enisa-news/spotlight-on-incident-reporting-of-telecom-security-and-trust-services

[2] https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

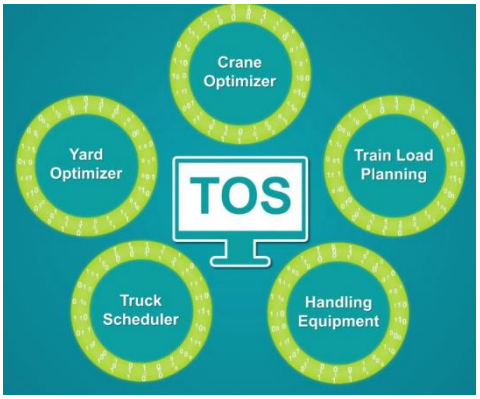
Supply Chain Attacks on Terminal Operating Systems (TOS)

Transport Sector, NCIIPC

Critical Information Infrastructure of Ports used as major supply line of international export and import, are attached with international terminal service provider. They have distributed data centres operating globally. Seaports operate many computerised systems for port management, loading and unloading of containers and cargo from vessels, shipping and storage at the port, customs payments, oceanic control and control systems, customer relationship data systems, physical security systems, and more.

The TOS system may be targeted in two ways in the cyberspace. The first cyber-attack vector is by a direct attack of the system from the Internet. This type of attack has been

observed in the form of ransomware attacks targeting vulnerabilities of Server Message Block (SMB), and has affected port operations globally. The second attack vector is through a supply chain attack, targeting one of the intertwined systems like software suppliers, third party system integrators or data service providers. The attacks can further penetrate other IT networks of the port, if the perimeter security devices are misconfigured, thereby affecting the functioning of port and resulting in cascading impact on business supply chain.



The attacks may also target the organisations who have been provided limited access to TOS for customer related activities. The attacker may exploit the unpatched systems of such interfaces to gain enhanced privilege. Phishing attacks on the vendors email can be a point of entry to get into the critical section of the organisation. These types of attacks can take a long time to detect as the traffic originates from trusted interfaces. Phishing is modus operandi of many threat groups and major concern of security teams of CII.

Phishing is modus operandi of many threat groups and major concern of security teams of CII.

Recently, as open source information indicates, attacks on information technology vendors in Saudi Arabia were reported to have been carried out, targeted by a cyber espionage group known as Tortoiseshell. This threat actor sneaked into the networks of IT service providers through supply chain attacks and their final goal was to steal confidential information from end customers. Cyber-attack on Iran's Shahid Rajaee Seaport was also reported.

References:

[1] https://www.jpost.com/cybertech/how-irans-shahid-rajaee-seaport-was-cyber-attacked-630158
[2] https://iimsr.eu/2020/05/20/how-was-irans-shahid-rajaee-sea-port-cyber-attacked/
[3] https://www.youtube.com/watch?v=gWPycombkkY

WordPress, Apache Struts Attract the Most Bug Exploits

Source: https://media.threatpost.com/

WordPress and Apache Strutsare most targeted by cyber-criminals in web and application frameworks. Most dangerous weakness type is input-validation bugs edged out cross-site scripting (XSS).Some specific types of bugs also saw a higher rate of weaponization. Information code injections, SQL injection and various command injections are most sought-after by cyber attackers for weaponization purposes. Lowest weaponization of vulnerabilities was observed in Python and JavaScript frameworks. JavaScript-based Node.js had a comparatively higher number of vulnerabilities than other JavaScript frameworks last year, Likewise, Django had 66 vulnerabilities, with only one weaponized.

Lowest weaponization of vulnerabilities was observed in Python and JavaScript frameworks.

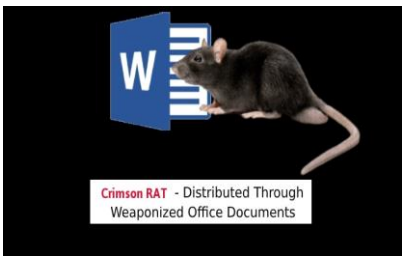
'Fake Fingerprints' Bypass Scanners with 3D Printing

Source: https://media.threatpost.com/

As per new research it has been found that it's possible to use 3D printing technology to create "fake fingerprints" which can easily bypass most of the fingerprint scanners used by popular devices, but this type of attack remains costly and time-consuming. 3D printing technology used by Cisco created different threat models on mobile devices. This fake fingerprint achieved about 80 percent accuracy on average, where the sensor was bypassed at least once. The MacBook Pro 2018 laptops fingerprint could be unlocked in 95 percent of the tests using fake fingerprint, but it failed each time when tested on Windows platforms. That does not necessarily mean that Windows devices are safer in terms of biometric authentication compared to other devices, according to the research. It might possible that the approach used by the fake fingerprint module failed to work on Windows platform.

This fake fingerprint achieved about 80 percent accuracy on average, where the sensor was bypassed at least once.

Malware Bytes



Hackers Attack Indian Financial Institutions with Crimson RAT

Source: https://gbhackers.com/crimson-rat

A new wave of APT campaign has been uncovered by researchers that target the Indian financial institutions with powerful Crimson RAT to exfiltrate sensitive data and to compromise network devices. It involves phishing email campaign that contains malicious attachment and sending the email to target organisation. The Crimson RAT infection process involves two different methods. In the first method a malformed email campaign hits the target with malicious link that points to an executable file which contains two ZIP files with an embedded document. Once the payload is executed on the victim's machine, it automatically checks the OS version of the system, reports to the command and control server and then drops the ZIP payload based on 32-bit or 64-bit version. Another method is spear-phishing campaign containing a malformed DOC file that has an embedded malicious macro. Once the victim opens the DOC file, the macro executes the RAT payload and loads the DOC file in the target system.

A malformed email campaign hits the target with a malicious link that points to an executable file which contains two ZIP files with an embedded document

TrickBot Bypasses Banking 2FA Protection via Mobile App

Source: https://www.bleepingcomputer.com

The TrickBot gang is employing a malicious android application that bypasses two-factor authentication (2FA) protection employed by various banks after stealing transaction authentication numbers. TrickMo has been designed by the TrickBot operators to intercept a good range of transaction authentication numbers (TANs), including mobile TAN (mTAN), one-time password (OTP), and pushTAN authentication codes, when installed on the victims' android devices. Initially TrickMo was spotted by CERT-Bund security researchers who said that TrickBot-infected Windows computers will ask the victims' online banking phone number and device types to prompt them to install bogus security app. Once installed, the app will forward text messages containing mTANs sent by the victims' banks to TrickBot operators, who can use them to create fraudulent transactions. Android operating systems include many dialog screens which require the approval or denial of app permissions, which receive confirmation from the user through tapping of a button on the screen. TrickMo uses accessibility services to spot and control a number of these screens and make its own choices before giving the user an opportunity to react.

Once installed, the app will forward text messages containing mTANs sent by the victims' banks to TrickBot operators, who can use them to create fraudulent transactions.

Targeted Attacks on Indian Government and Banking Sector

Source: https://www.zscaler.com

In April 2020, ThreatLabZ found several instances of targeted attacks on Indian Government establishments and banking sector. Emails were sent to organisations, such as Reserve Bank of India, IDBI Bank, National Bank for Agriculture and Rural Development (NABARD) with archive file attachments containing JavaScript and Java-based backdoors. Java based RAT provided functionalities similar to the Java script based backdoor in this attack. This threat actor has a specific interest in India based organizations and the content of the emails indicates a good knowledge of topics relevant to each of the targeted organisations. The backdoors used in this attack are uncommon, such as JsOutProx, which has only been observed in the wild once before in December 2019. Zscaler said, "The ZscalerThreatLabZ team will continue to monitor this campaign and as well as other campaigns to help keep our customers safe".

This threat actor has a specific interest in India based organizations

Malware Delivered to Sophos Firewalls

Source: https://www.securityweek.com, https://gbhackers.com

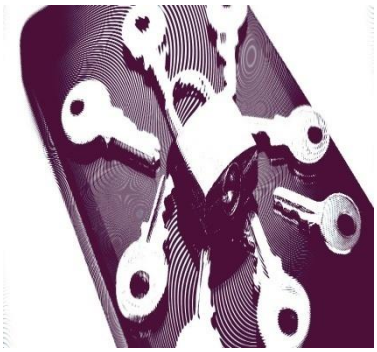
Cyber Security Company Sophos informed its customers that it

After determining the components and impact of the attack, Sophos deployed a hotfix to all supported XG Firewall/SFOS versions.

has patched a zero-day vulnerability that has been exploited to deliver malware to its XG Firewall appliances. According to the company, the attack was aimed at systems with the administration service or user portal exposed to the internet. The attackers would try and exploit the security hole to download malware that would allow them to exfiltrate data from the firewall. This data could include usernames and password hashes for the local drive administrators, portal admins and user accounts set up for remote access. Passwords associated with external authentication systems such as AD and LADP were unaffected. After determining the components and impact of the attack, Sophos deployed a hotfix to all supported XG Firewall/SFOS versions. Users are recommended to apply the hotfix that eliminates the SQL injection vulnerability, for compromised devices it is recommended to reset the passwords for all local user accounts.

Cerberus Malware can Bypass 2FA, Unlock Devices Remotely

BFSI Sector, NCIIPC



It was also discovered that Trojan now has TeamViewer-based Remote Access Trojan (RAT) capabilities.

Advanced Banking Malware Cerberus having Remote Access functionality is capable of stealing victims' Google Authenticator two-factor authentication (2FA) codes used as an additional layer of security when logging into accounts. Google Authenticator is Google's alternative to SMS-based two factor authentication, which uses a data connection to send one-time passcode (OTP) via text messages. SMS-based messages can be diverted because they are sent using an external carrier network, while a local app to get codes is seen as a safer alternative. However, researchers have discovered a sophisticated Cerberus banking Trojan sample which can log and steal information from Google Authenticator. "While the app is in running mode, the Trojan can access the information of the interface and have ability to send it to the Command & control server. These stolen codes can be used to evade the additional 2FA security layer on online services such as banks, email services, messaging apps, and social media.

Fully operational RAT module: It was also discovered that Trojan now has TeamViewer-based Remote Access Trojan (RAT) capabilities. The RAT service is able to pass through the file system of the device and download its contents. It can also launch TeamViewer and setup connections to it, providing threat actor full remote access of the device. This new module can be used by Cerberus' operators to manage apps on infected Android devices, change device's settings, as well as use any of the apps installed just like the device owner. The Android malware sample also comes with a screen-lock grabbing feature that uses overlays, making it possible for the attackers to use the built-in RAT to unlock their victims' Android devices remotely. Having an in-depth target list including institutions from all over the world, combined with its new

capability, malware is a dangerous for financial services providers offering online banking services.

References:

[1] https://www.bleepingcomputer.com/news/security/cerberus-android-malware-can-bypass-2fa-unlock-devices-remotely/

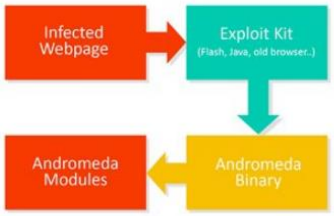
Andromeda Botnet

Power & Energy Sector, NCIIPC

Andromeda botnet also known as Gamarue, can allow remote, unauthorized access into the systems by injecting malware and creating backdoors. The malware mainly targets the Windows operating systems to create a network of infected computers. The botnet is used to distribute other malware families with which Andromeda is associated with. It is a highly modular platform for malicious activity. While it consists of key loggers, rootkits, anti-VM, anti-debugging and proxy features, it is mostly used as a method to establish a reliable backdoor to further deliver additional malware. There are four phases in spreading this malware:

- Downloader retrieves spam engine
- Exploit kit performs drive-by install
- Execute spammer
- Compromised websites lead to exploit kit

Challenges: The main challenge is to ensure the safe, reliable and continuous operation of control systems and safety networks, by securing them from Andromeda Trojan being injected from less trusted external networks. It is also essential to provide real-time access to operations data to enterprise users. One has to prevent the botnet from distributing other malwares like DDoS malware, ransomware, which can lead to disruption in applications and OT systems of Power and Energy sector or locking of critical systems by ransomware.



Risks to Power and Energy systems from Andromeda vulnerability: Andromeda botnet can perform different commands from its control servers for downloading and executing files, performing remote shell, and uninstalling itself from Power and Energy utility systems & servers. Andromeda botnet is distributed via malicious emails containing attachments or links to compromised websites hosting Exploit Kit content.

Recommendation to prevent spread of Andromeda Botnet:

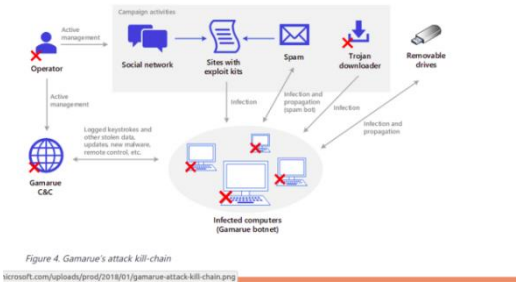


Figure 4. Gamarue's attack kill-chain

- Never allow macros to be run on any document that appears to be a suspicious email and block malicious attachments being run.
- The infection is triggered when a user uses vulnerable software downloaded from a compromised site, hence, stay away from compromised sites that host malicious software installers which can spread various types of malware and ransomware.
- Extra care may be taken while opening emails or social media messages received from unknown users.
- Never download software from websites other than reputed sources or directly from the original program developers.

References:

[1] https://www.theregister.com/2017/12/05/international_team_takes_down_virusspewing_andromeda_botnet/

[2] https://blog.malwarebytes.com/detections/backdoor-andromeda/

[3] https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ANDROMEDA

[4] https://www.microsoft.com/security/blog/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/

[5] https://www.2-spyware.com/remove-andromeda-trojan.html

New PoetRAT Hits Energy Sector with Data-Stealing Tools

Source: https://threatpost.com/

PoetRAT is an emerging malware that targets the energy and government sectors with different tools that are aimed at stealing credentials and exfiltrating sensitive data. It is circulated through three separate documents. The first document which contained unreadable content, is named "C19.docx" likely a reference to COVID-19. The second is named "Azerbaijan_special.doc". All files are located on a server tied back to: http://govaz.herokuapp.com/content/section_policies.docx. In all these documents, once the macros are enabled, a Visual Basic script dropper is executed. The script loads its own document into memory, which is a ZIP file ("smile.zip") that contains a Python interpreter, as well as a Python script that is the RAT. Meanwhile, the Word macros also

unzip and execute a main script called "launcher.py" which checks the environment. The RAT itself is comprised of two main scripts i.e "frown.py" responsible for the communications with the command and control (C2) and "smile.py" responsible for execution of the C2 commands. These commands retrieve system information, take screenshots, copy, compress and hide files and more.

Oil and Gas Firms Targeted with Agent Tesla Spyware

Source: https://threatpost.com/oil-and-gas-agent-tesla-spyware/154973/

Agent Tesla Spyware is a .Net-based and commercially available info-stealing program active since at least 2014. Many energy companies have been targeted by the attackers with Agent Tesla spyware as seen in recent spear phishing emails with malicious attachments. The malware was designed to collect credentials and various sensitive information and send all data back to a Command and Control (C&C) server at smtp[:]//smtp.yandex.com:587. In first campaign, the attackers mimicked EnPPI (Engineering for Petroleum and Process Industries) to request bids for equipment and materials, as part of the Rosetta Sharing Facilities Project, on behalf of gas company Burullus. The emails sent as attachments archives designed to inject Agent Tesla onto the victims' machines. In the second campaign, the adversary pretended to be a shipment company and leveraged legitimate information about a chemical/ oil tanker to focus on victims in the Philippines. This can be part of a growing threat against industrial organizations, including oil and gas companies, that rely heavily on remote access to keep up their operations.

In the second campaign, the adversary pretended to be a shipment company and leveraged legitimate information about a chemical/ oil tanker

Zoom Vulnerability Exploit to Record Meetings

Source: https://securityboulevard.com/

Recently a flaw in the Zoom application has been identified that enables threat actors to record Zoom sessions and capture chat text without the knowledge of the meeting participants. The Zoom malware is able to perform this activity even when the host has disabled recording functionality for the participants. The trigger malware injects its code into a Zoom process with no interaction from the user and even when the host has disabled the participants to record the meetings. When recording in this manner, the malware fully controls the output and none of the participants are aware that the session is being recorded.

None of the participants are acknowledged that the session is being recorded while the malware fully controls the output

This vulnerability is similar to an IDN Homograph attack and has the same risks.

Zero-day Vulnerability in SaaS Services Exploited

Source: *https://cyware.com/*

Cybercriminals are exploiting a zero-day vulnerability in SaaS services to register malicious generic top-level domains and subdomains that look the same as legitimate sites. The impacted SaaS services include Amazon, Google, and Digital Ocean. The purpose behind this is to launch phishing attacks against organizations. Demonstrated by Matt Hamilton, a principal security researcher at Soluble, this vulnerability is similar to an IDN Homograph attack and has the same risks. He highlighted that an attacker could register a domain or subdomain that appears visually identical to its legitimate counterpart and perform social-engineering or insider attacks against an organization. Verisign, the authoritative registry for the .com, .net, .edu, and several other generic top-level domains (gTLDs) has fixed the flaw and now restricts the registration of domains using these homoglyph characters. In addition, it has changed domain name registration rules by updating the table of allowed characters in newly registered domains. Soluble in partnership with Bishop Fox has also reported the vulnerability to the vendors of SaaS services. A patch for the vulnerability is yet to be released by the vendors.

Entire network was brought down despite the efforts of the IT department, with PCs overheating, freezing, and rebooting because of blue screens, and Internet connections slowing down because of Emotet devouring all the bandwidth

Emotet Took Down a Network by Overheating All Computers

Source: https://www.bleepingcomputer.com

Microsoft has stated that an Emotet infection was able to take down an organization's entire network by maxing out CPUs on Windows systems and bringing its Internet connection down, after one employee was tricked to open a phishing email attachment. The virus avoided being detected by antivirus solutions through regular updates from an attacker-controlled command-and-control (C2) infrastructure, and spread through the company's systems, causing network outages and shutting down essential services for nearly a week. The Emotet payload was delivered and executed on the systems of Fabrikam, a fake name Microsoft gave the victim in their case study. Within 8 days since that first booby-trapped attachment was opened, Fabrikam's entire network was brought down despite the efforts of the IT department, with PCs overheating, freezing, and rebooting because of blue screens, and Internet connections slowing down because of Emotet devouring all the bandwidth.

Guest Article

Identifying Critical Infrastructure in a Global Tier-1 ISP

Lt. Col. A J Vijayakumar (Retd), CISSP

A global Tier-1 Internet Service Provider that provides 24x7 voice

and data connectivity to international customers has literally thousands of individual pieces of communication equipment, which includes fiber-optic submarine cables, transmission equipment, routers and switches, voice switches, media gateways, and so on. The Internet services provided by such telecom enterprises have high national economic value, since any disruption of internet traffic will affect large sections/regions of the country.

Cyber security in telecommunication enterprises typically focusses on ensuring that the most critical equipment is provided the highest degree of protection so that the security investment is optimally utilised in protecting the most critical assets of the enterprise. Identification and prioritisation of the most critical equipment helps in reducing the overall Measure of Risk, which is achieved by focusing the Risk Assessment activities on a smaller (and manageable) number of critical equipment rather than on the entire list of thousands of telecommunications equipment.

This article proposes a mechanism for categorising equipment on the basis of their criticality within a global carrier grade Tier-1 Internet Service Provider, which has advanced submarine cable networks and a Tier-1 IP network with connectivity to multiple countries across the globe, hundreds of Points of Presence (PoP) and large global data centres.

Complexity of large numbers, varieties of technologies and vendors: Any large global telecommunications enterprise will have 15000 to 25000 Information Systems as part of its infrastructure, each uniquely identified by an IP address. This excludes end user's equipment. The infrastructure complexity arises from the large variety of equipment for different functionalities from multiple manufacturers and a global geographic spread spanning across continents.

Need for identifying the critical infrastructure: It is well known that a Risk Based approach is the most common practice to manage cyber security in enterprises. It involves conducting technical as well as operational (or process) Risk Assessment. The Measure of Risk (MoR) is a function of four factors, namely the asset value, threats, vulnerabilities and likelihood of the threats exploiting the vulnerabilities. As the assets, which are of greater value have greater risk, the enterprise must have a clear list of critical assets identified from amongst the overall infrastructure. The following questions will help determine the criticality:

- Which equipment, whose compromise or failure will impact the services the greatest?
- Are most of the manufacturers covered from amongst the critical equipment?

Lt. Col. A J Vijayakumar (Retd) has been with Tata Communications Ltd. as a Chief Information Security Officer (CISO) for nearly 9 years out of a total of 11 years of service in the company

- How can Risk Assessment of these be carried out in a realistic time frame, say at least once a year?

Based on the response to above queries, one can classify equipment into 5 categories, namely 'Most Critical', 'Critical', 'High Value', Important and 'Others'. This is applied on the following classes of equipment:

- IP Equipment (Routers – Access, Aggregation and Core Routers): The Core routers assume the greatest importance, as this is where the traffic from aggregate routers collect. These mostly consist of high-speed switches of 100+Gbps, located in Tier-1 cities. Aggregate routers are of next importance as this collect traffic from access routers. These are medium capacity switches, normally located at Tier-2 cities or within a large metro. Access routers are of lesser importance compared to the other two types mentioned above.
- Voice Equipment (Voice Switches and Media Gateways for VoIP): Voice traffic nowadays is mostly carried on the IP network. The most critical equipment is Media Gateways that bring in traffic from pure voice switches and convert to VoIP to feed into the IP network.
- Transmission Equipment (Dense Wavelength Division Multiplexing Equipment): DWDM equipment at locations of Core Routers or at Cable Landing Stations (CLS) are the most critical.
- Operations Support Systems (OSS) and Business Support Systems (BSS) Systems: OSS and BSS are important for an enterprise for correct measurement and billing of customers, as well as for smooth management operations of the network.
- Security Devices (IDS, Firewalls, Web Filters, Access Control Servers etc.): The devices, which provides functions to the core network and impact organization-wide resilience are the most critical.
- Corporate IT (Web Servers, Mail Servers, Applications, Databases): Corporate IT and Security systems are critical to the enterprise.

Let's say the number of devices (each defined by an IP address) excluding the end-user systems is 20000. Out of these approximately 10000 IPs reside within the country, as most corporations also have assets outside the country. Out of these approx. one-third, say 3000 IP addresses fall in the category of access/aggregation/core equipment. Out of these, the 'Critical' systems about 500 and 'Most Critical' around 150, totaling to around 650. About 1200 fall into the 'High Value' category and the remaining in the 'Important' category. This is

given in tabular form below.

Most national agencies demand that telecommunication enterprises carry out third party audit once a year. The 'most critical' IP addresses could be put through both external and internal audits once a year, the 'critical' through internal risk assessments every year, and the 'High Value' and important assets be subjected to internal risk assessments once every 3 years in a rotation.

Type of Equipment	**Sub-Type**	**Critical (Approx.)**	**Most Critical (Approx.)**	**Description & Rationale**
IP Devices	Core Routers	30	10	These form the backbone of the ISP within the country, Typically Tier-1 cities
	Aggregation Routers	60	20	For smaller PoPs (Tier-2 Cities)
	Access Routers	120	40	For Tier-3 Towns
Voice Equipment	Voice Switches/ Media Gateways	50	15	Most Traffic is VoIP, which runs over the IP Network
Transmission Equipment	Transmission Switches	60	15	Fibre-Optic(DWDM switching)equipment
OSS / BSS	CDRs, Billing System	60	15	Call Data Record Servers, billing &provisioning systems.
Corporate IT	Servers, Applications, Databases	60	15	Mail Servers, SAP/ERP Servers
Corporate Security	Access Control Servers (ACS), Traffic Monitoring and Security devices.	60	20	Firewalls, IDS, DDoS Monitoring Collectors, Scrubbers etc.
	Total	500	150	

It is extremely important to categorise telecommunication equipment on the basis of criticality, both enterprise-wide and nation-wide. The rationale for arriving at a particular classification has been suggested in the paragraphs above. Telecom enterprises vary in size, geographical spread and the variety of services they offer. Each enterprise must therefore categorise the importance/criticality of the equipment, suited its own environment, so that the right amount of attention can be given both from an enterprise as well as national perspective.

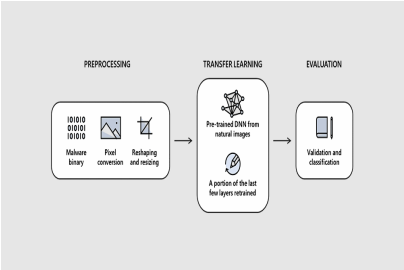
Learning

To maintain a secure perimeter, it is important for CISOs to understand their RF attack surface.

Radio Frequency: An Invisible Espionage Threat to Enterprises

Source: https://www.helpnetsecurity.com/

Radio-based attacks have been conducted by foreign governments, competitors and cyber criminals on enterprises. Radio Frequency (RF) devices are mainly used as their entry points for these sophisticated attacks. To gain access to company networks and secrets, cell phones, health performance monitors and IoT infrastructure devices offers unmonitored threat surfaces to launch an attack. To keep the threats at bay, government facilities with valuable secrets have policies to exclude RF devices. Vulnerabilities that are detected in recent radio-based device include SweynTooth, the Phillips Hue, BleedingBit, MouseJack, and KeySniffer which affect billions of devices. To maintain a secure perimeter, it is important for CISOs to understand their RF attack surface. Firstly, what devices are operating in their radio space and whether that traffic is encrypted or not, all should be found out by organizations. Then solutions that can detect and accurately locate individual cellular devices in addition to providing accurate locations for the more common Wi-Fi, Zigbee, Bluetooth and BLE-based devices should be considered by CISOs.



The project relied on a new technique that converts malware samples into grayscale images

Microsoft and Intel Project Converts Malware into Images

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

A new research project that explored a new approach to detect and classify malware has been recently collaborated by Microsoft and Intel. It is called STAMINA (STAtic Malware-as-Image Network Analysis), the project relied on a new technique that converts malware samples into grayscale images and then the image for textural and structural patterns specific to malware samples is scanned. Researchers then took this one-dimensional (1D) pixel stream and converted it into a 2D photo to analyse using normal image analysis algorithms. To train the original DNN algorithm, researchers used 60% of the known malware samples, 20% of the files to validate the DNN, and the other 20% for the actual testing process.

How to Mitigate Windows Font Parsing Zero-Day Bug via GPO

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

Adobe Type Manager Library of Microsoft is exploited by a Remote Code Execution (RCE) zero-day vulnerability found in Windows. Here, Windows 7 is very much affected. Windows 10 allows limited permissions and code execution capabilities; thus, a successful attack can only occur in an App Container sandbox context. An attacker can open the malicious crafted

documents or view them via the Windows Preview pane. But it doesn't mean that the Outlook Preview Pane is an attack vector. Microsoft has suggested the disabling of Preview and Details panes in Windows Explorer, disabling the Web Client service, and renaming the vulnerable library (ATMFD.DLL) through a strong Group Policy Objects which are needed to prevent such attacks in Windows. Currently, implementation of Group policy object is not an easy task in an enterprise AD environment. When Microsoft releases a patch for the actively exploited RCE vulnerabilities, above policies should be revoked which is also a cumbersome task.

Microsoft suggested to disable the Preview and Details panes in Windows Explorer, disable the Web Client service, and rename the vulnerable library

Cyber Security During COVID-19: Stay Vigilant Stay Safe

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

As Covid-19 pandemic disturbing global health, economic, political and social systems, there's another unseen threat rising in the digital space: the risk of cyber-attacks. A major factor arising from the actions of these threat actors are fake COVID-19 websites, phishing emails and malwares, which may promise a cure or treatment in exchange for personal information. Following are the threats users shall be aware off and take case

A major factor arising from the actions of these threat actors are fake COVID-19 websites, phishing emails and malwares, which may promise a cure or treatment in exchange for personal information.

Phishing Domains: Indian Cybercrime Official released a list of potentially Dangerous Coronavirus related domains to be aware off.

Malware Threats: Cybercriminals are using a phishing campaign which informs victims that they have come in contact with someone diagnosed with COVID-19 and tricks them into downloading malware.

How you will protect yourself from these phishing and malware attacks?

- Be aware of fraudulent emails claiming to be from expert. They might say that have information about virus.
- Do not click on any link from unknown sources. They could download malware and viruses on your computer or device.
- Check the true destination of the link by hovering the pointer over the hyperlink
- Disconnect or delete any call or messages that ask for your personal or financial details
- Do not open attachments or click on links in emails, text messages or social media messages from strangers

Work from Home (WFH): There is an increase in the number of cyber-attacks on computers, routers and unprotected home networks used by employees who have switched to remote working due to the spread of COVID-19.

Following security measures to be employed while working from home:

- Use strong and unique password on every account and device – consider two factor authentications wherever applicable (2FA)
- Update VPN, network devices, and devices being used to remote work environment with latest software patches and security configuration.
- To share files only use the software which Company would typically use. Refrain from using personal email ID or 3rd party services.
- Do not allow sharing of work computers and other devices

AI, ML, NN, DL: Interdependencies and SOC Applications

Director, NSAC, NCIIPC

Machine Learning (ML) is subset of AI (Artificial Intelligence), the terminology used for simulation of human intelligence (like Turing Test) processes by machines whereas ML is a way to use the concept of AI with little supervision from humans except in terms of initial algorithm and data. Deep Learning (DL) is sub-field of Neural Network (NN). These NN are set of algorithms to mimic human brain. DL is sub-branch of ML under NN which trains and learn from vast amount of data powered by NN. If data is considered to be a crude oil, DL can be treated as oil refinery converting crude oil into final finished product. "Data is Gold" not only from the perspectives of Governance, Businesses, Cyber Criminals but also for SOC (Security Operation Centres) teams which, as per NIST cyber security framework, help them to identify, protect, detect, respond and recover from any cyber intrusion. For SOC teams to have a holistic view, data from different devices viz. endpoints, network devices, perimeter protection devices, authentication/mail/web/AV servers etc. is required at centralized location for IR (Incident Response)/Forensics activities and pinpointing IOAs (Indicator of Attacks), IOCs (Indicator of Compromises), cyber kill chain, TTPs (Tools Techniques Procedures).

If data is considered to be a crude oil, DL can be treated as oil refinery converting crude oil into final finished product.

The entire data of a big enterprise network with global presence can be in GBs/TBs, and can be a nightmare to the SOC team for manually carrying in depth analysis. AI (Artificial Intelligence), ML (Machine Learning), NN (Neural Network), DL (Deep Learning) comes to the rescue of these SOC teams, to assist them through technology to do the automation to most of the daily mundane-cum-repetitive tasks of threat hunting for identification of malicious anomalies in the aggregated massive pile of data.

The primary aim for amalgamation of these components in SOC is to reduce MTTD (Mean Time To Detect) and MTTR (Mean Time To Respond/Remediate) under the dwell time of the attacker.

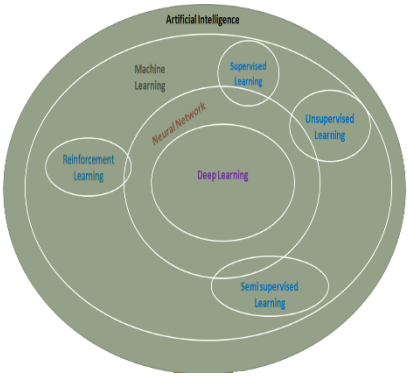


Figure 1: Interrelation of AI, ML, NN and DL

- Interrelation between AI, ML, NN, DL: AI, ML, NN, DL are the components used to complement the SOC in terms of maturity in handling the daily operations. Interrelation of the mentioned components is highlighted in *Figure 1*. AI is super set of ML, NN, DL and is present in most of the next generation cognitive computing SOC (NGC2SOC). However, DL is the subset of NN, which is aimed towards reducing the false positives in addition to automation of threat hunting.
- Machine Learning and classifications and applicability to SOC: ML is used in conjunction with Big Data. Big Data is characterized by 3 Vs viz. Volume, Variety and Velocity at which the data must be processed uses ML.

ML is used in conjunction with Big Data. Big data which is characterized by 3 Vs viz. Volume, Variety and Velocity at which it has to be processed uses ML.

As depicted in *Figure 1* ML is sub-set of AI and is further categorized as highlighted in *Figure 2*.

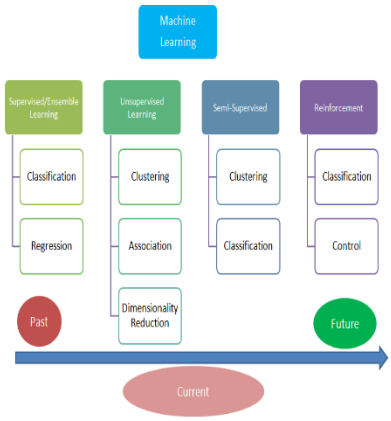


Figure 2

- Supervised Learning: This learning involves labelled data in SOCs with applications like spam mail detection. Classification is discrete process whereas regression is continuous process.
- Unsupervised learning: This involves the clustering of similar type of event based on traffic. Malicious botnet traffic detection is possible through clustering analysis. Clustering identifies similar cases while association identifies similarity.

Supervised Learning involves the labelled data in SOCs with applications like spam mail detection. Classification is discrete process whereas regression is continuous process

- Reinforcement Learning: This is a reward-based learning system, useful in performing certain actions in particular state like DDoS, Vulnerability Scan, SOC triage.

Conclusion: SOC is central technical operational unit working 24x7 monitoring, analysing, identifying, assessing, forecasting and defending malicious intrusions in the organisation's enterprise network. Staff at NGSOC/NGC2SOC by design is required to handle big data in close coordination with threat hunters, data scientists, analysts, network/IT teams, Audit/IR/VAPT teams and management. AI, ML, NN, DL are the interdependent components which not only provides the automation to the mentioned SOC but also helps in some of the mentioned traits:

- Striking balance between false negatives and false positives with aim of reducing unknown unknowns.
- Behavioural profiling for Accurate threat prediction/forecast
- Identifying TTPs (Tools, Techniques, Procedures)
- Cross-sectional threat modelling
- Speeding accurate IR (Incident Response)/Threat Mitigation

SOC with amalgamation of AI, ML, NN, DL may further help in developing maturity in conjunction with some of the available matrix like SOC-CMM (Capability Maturity Model) having level 0 to level 5 broadly based on 5 domains viz. Business, People, Process, Technology and Services.

SOC with amalgamation of AI, ML, NN, DL may further help in developing maturity in conjunction with some of the available matrix like SOC-CMM (Capability Maturity Model) having level 0 to level 5 broadly categorized in 5 domains viz. Business, People, Process, Technology and Services.

References:

[1] https://www.blackhat.com
[2] https://www.sans.org
[3] https://www.soc-cmm.com
[4] https://www.ida.org
[5] https://www.researchgate.net
[6] https://www.techbeacon.com
[7] https://www.universalreview.org
[8] https://www.researchgate.net
[9] https://www.towardsdatascience.com
[10] https://www.securityintelligence.com

Business Continuity Plan for CII Organisation

Transport Sector, NCIIPC

Technological development has made Information and Communication Technology (ICT) an in-separable part of business processes running on information infrastructures in critical sectors. Organizations have also become more dependent on resilient, secure and safe IT infrastructures. The dichotomy of boon and bane of technology has persistent for humankind ever since technological evolutions. The technological development cyber has created numerous opportunities for solving problems in efficient and cost-effective manner. The other side of cyber is an environment of cyber-attacks on IT infrastructure of the small, medium and large scale organisations of every sector. Increased and sophistication of cyber-attacks on an organization's Critical Information Infrastructure (CII) has impacted the delivery of services that are essential in terms of protecting nations four pillars of Security, Economy, Healthy and Safety. These attacks result in unplanned downtime and loss of critical information/data that may originate from various sources. The reason behind such knee jerk reaction is that organizations are unable to sustain, due to insufficient or below standard Business Continuity Plan (BCP) that has not been executed and tested on ground. As per the definition of ISO22301, the broader ISO standard for business continuity, BCP is "Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption". [1] Further, Section A.17.1 of ISO 27001 has stated that an organization shall embed information security continuity in its business continuity management systems. ISO 27031 is a mechanism to implement the principles of ISO 22301, it provides detailed guidance on establishing continuity of ICT elements. Business continuity entails the planning and preparation for such unexpected adverse situations in order to avoid disruption of the activities of an organisation and maintain availability, integrity, and security. NCIIPC Control Guideline v2.0 states regarding BCP that "These controls are essential to ensure minimum downtime, as well as to ensure that the restoration process factors in, and overcomes the initial vulnerabilities, or alternatively isolates infrastructure compromised by attackers, to ensure graceful degradation / minimum maintenance of Service provided by the CII."[2]If we take an example of Power/Transport Sector infrastructure of the nation. Any disruption in these sectors due to Crisis / Disaster creates hardship to the human beings, as every aspect of human life is directly or indirectly. The electrical infrastructure used in these sectors are SCADA / ICS based which are cyber physical systems and if BCP to handle the cyber disruption

needs to be taken in to account.

Disaster Recovery / Business Continuity Planning (BCP) Controls prescribed by NCIIPC

- DR1: Contingency Planning
- DR2: Data Back-up and Recovery Plan, Disaster Recovery Site
- DR3: Secure and Resilient Architecture Deployment

Defining BCP for CII:

- Understand organization CII and its unique requirements.
- Identify and define the needs and expectations of all the stakeholders supporting CII.
- Careful statement of purpose and scope of plan i.r.o. critical IT elements.
- Consider legal and regulatory requirements when designing BCP.
- Involve higher management / leadership for approval of organisation's BCP
- Necessary resources for CII to cater separately or priority define for resource allocation.
- Competence requirements of the people under an organisation's control who have an impact on its performance
- Awareness of their responsibilities for CII's BCP.
- Establishing communication procedures to internal as well as external stakeholders for pre, during and post emergency/disaster,
- Identifying critical activities to be recovered and timescales for their recovery.
- Ensuring plans are easily accessible and copies kept on and off site.
- Proper documentation of roles of individuals
- Building up strategies for communicating with staff, Document BCP and control distribution.
- Review of documents and procedures on regular interval of time.

References:

[1] https://www.iso.org/home.html

[2] https://nciipc.gov.in

[3] https://www.pace.edu/security-emergency-management/business-continuity-planning

[4] https://www.google.com/search?q=Business+continuity+life+cycle+images

[5] https://www.google.com/search?q=contingency+planning+images

Rail and Metro Cybersecurity

Transport Sector, NCIIPC

Transportation system for regional, inter-city, urban mass transit and passenger rail systems are all encountering threat vectors that are affecting the entire transportation industry in general. These threats are due to the sector's increasing reliance on networked control and remote access automation systems for more efficient operation at a lower cost. The large geographical spread of railway systems, that is supported by multiple providers and the large number of people involved in operating and maintaining those widespread systems offer attackers an almost unlimited number of attack vectors. Critical railway system:

- External Zone: Access Control / Intrusion Detection, Passenger Information System and Advertising & CCTV.
- Operational Zone: Dispatch/ATS, SCADA, Traction Power, Trackside Equipment and Traffic Controller Interface.
- Critical Zone: Signaling/Automatic Train Protection (ATP), Communication Based Train Control (CBTC)

Threats to Rail System and Key encounters to protected railways infrastructure: The Characteristics of railway infrastructure make them objectives for cyber-attacks due to the following:

- High degree of co-ordination between IT and Operational Technology (OT)
- Distributed architecture of systems/networked deployed.
- Long lifecycles for equipment and certification processes. Once a component of the system is certified, it might be outdated from a cybersecurity angle in particular, considering the evolving threat landscape.
- Diversity of supply chain and technology
- Ignorant / untrained cyber security personnel.

Recommendations: Cyber security is a critical requirement, but is not given adequate attention by the management since it is not a profit generating activity. However, it is important to know that cyber-attacks can significantly affect the profitability of the railways. Cyber security must be incorporated at the initial

phases of any project. The organisations must also have reliable governance, risk management strategies and compliance monitoring.

Reference:

[1] https://cyberstartupobservatory.com/rail-cybersecurity-where-is-the-industry-now/

Securing the Enterprise Virtual Private Network

S&PE Sector, NCIIPC

Due to the Corona virus pandemic, employees from many organizations have been advised to work from home. As there is an increase in number of employees working from home, a way to secure their communications with the corporate network is needed. One of the solutions is Virtual Private Network (VPN). A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Simply VPN enables communication through secure online servers using encryption of data. With large number of organizations using VPN, attackers are finding vulnerabilities to target organizations for various Cyber-attacks. There are security risks associated with VPNs. These includes:

- VPN hijacking, in which an unauthorized user takes over a VPN connection from a remote client.
- Man-in-the-middle attacks, in which the attacker is able to intercept data.
- Weak user authentication.
- Split tunnelling, in which a user is accessing an insecure Internet connection while also accessing the VPN connection to a private network.
- Malware infection of a client machine, granting too many network access rights.
- DNS leak in which the computer uses its default DNS connection rather than the VPN's secure DNS server.

To address these risks, enterprises should consider additional VPN security features when choosing a VPN product.

Best practices for using VPNs:

- Update VPNs and network infrastructure devices with the latest software patches and security configurations.
- Organizations should advise their IT team to increase scrutiny of unauthorized activities using log analysis, detect

attacks in timely manner and respond to incidents.

- Alerting employees of increased phishing attempts.
- Enabling Multi-factor Authentication (MFA) for VPN accounts.
- IT personnel should test the VPN server for mass usage.

References:

[1] https://www.esecurityplanet.com/network-security/vpn-virtual-private-network.html

[2] https://www.us-cert.gov/ncas/alerts/aa20-073a

[3] https://www.zdnet.com/article/covid-19-with-everyone-working-from-home-vpn-security-has-now-become-paramount/

Vulnerability Watch

Siemens Industrial Devices Affected by 'SegmentSmack'

Source: https://www.securityweek.com, https://ics-cert.kaspersky.com

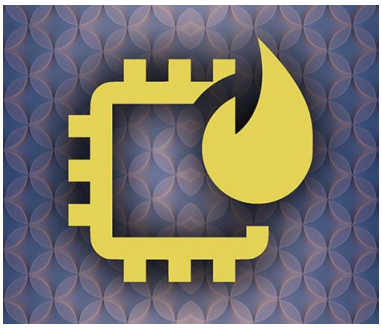
Several Siemens products were affected by SegmentSmack (CVE-2018-5390) and FragmentSmack (CVE-2018-5391) vulnerabilities. The vulnerable products include IE/PB-Link devices, RUGGEDCOM routers, SCALANCE firewalls, SIMATIC CP communications processors, the SINEMA Remote Connect Server, etc. The SegmentSmack and FragmentSmack vulnerabilities have the CVSSv3 Base Score of 7.5 that were identified back in 2018 and are due to flaws in the Linux kernel's TCP stack. For some of the affected products, the vulnerabilities can be fixed by installing updates.

The SegmentSmack and FragmentSmack vulnerabilities are due to flaws in the Linux kernel's TCP stack.

Starbleed Vulnerability: Attackers Can Gain Control Over FPGAs

Source: https://www.helpnetsecurity.com

Field Programmable Gate Arrays (FPGAs) are flexibly programmable computer chips that are considered very secure components in many safety-critical applications such as



Since the bug is integrated into the hardware, the security risk can only be removed by replacing the chips.

cloud data centers, mobile phone base stations, encrypted USB-sticks and industrial control systems. The advantage of these chips lies in their reprogrammability compared to conventional hardware chips that have fixed functionalities. A critical vulnerability was discovered in these chips called Starbleed. The update and fallback feature in the FPGA revealed itself as a weakness and gateway. The advantage of individually reprogramming the chips turned into a disadvantage. If an attacker gains access to the bitstream, he also gains complete control over the FPGA. Intellectual properties included in the bitstream can be stolen. It is also possible to insert hardware Trojans into the FPGA by manipulating the bitstream. Thus, attackers can gain complete control over the chips and their functionalities via this vulnerability. Since the bug is integrated into the hardware, the security risk can only be removed by replacing the chips.

The PPP runs with high privileges and works in conjunction with kernel drivers.

Critical Vulnerability in Point to Point Protocol Daemon (pppD)

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

pppD is used to manage the network connections in Unix based operating systems and is also used to manage broadband connections such as DSL, if (PPPoE) or (PPPoA) is used. Critical buffer overflow vulnerability (CVE-2020-8597) was discovered in the pppD that let remote attackers exploit the Linux systems remotely and gain root-level privileges. This vulnerability resided in the Extensible Authentication Protocol (EAP) packet processing in pppD. It has a CVSS 3.0 Base Score of 9.8. The versions affected are 2.4.2 through 2.4.8. The Linux distributions that were affected by this vulnerability are- Debian GNU/Linux, Fedora Project, Red Hat, SUSE Linux and Ubuntu.

The SafeBIOS Events &IoA is designed to identify endpoint threats at the BIOS level by using behavior-based detection technology.

New Dell Utility Alerts Security Teams of BIOS Attacks

Source: https://www.securityweek.com/

Dell announced the launch of Dell SafeBIOS Events & Indicators of Attack, a utility designed to alert IT and security teams about BIOS configuration changes. SafeBIOS Events &IoA is designed to identify endpoint threats at the BIOS level by using behavior-based detection technology. The utility monitors the BIOS for any configuration changes and analyzes them to determine if they could be part of an attack. When a potential exploit is detected, the organization's IT or security team is immediately notified in their management console, enabling them to take quick action before too much damage can be done. "Securing the BIOS is particularly critical because compromised BIOS can potentially provide an attacker with access to all data on the endpoint, including high-value targets like credentials. In a worst-case scenario, attackers can leverage compromised BIOS to move within an organization's network and attack the broader IT infrastructure," said Dell.

Patching Pulse Secure VPN Not Enough to Keep Attackers Out

Source: https://www.securityweek.com

U.S. Cybersecurity and Infrastructure Security Agency (CISA) have warned patching vulnerable enterprise VPNs from Pulse Secure is not enough to keep out malicious actors who have already exploited the vulnerability. A total of 10 vulnerabilities were reported to Pulse Secure in March last year, and patches for them were released. The most severe of these issues, was CVE-2019-11510, which can be abused by an unauthenticated, remote attacker to execute arbitrary code. The vulnerability is targeted with crafted requests for files that allow for Credential Dumping plaintext passwords from the VPN appliance. Cybercriminals were observed connecting to compromised environments using Tor and virtual private servers (VPSs) to avoid detection. It is strongly recommended that organizations upgrade their Pulse Secure VPN to the corresponding patches for CVE-2019-11510 along with changing passwords for all Active Directory accounts, including administrators and services accounts.

Flaws in ABB DCS Causes Disruption in Industrial Environments

Source: https://www.securityweek.com

Critical vulnerabilities have been found in the ABB System 800xA distributed control system (DCS) and some related products. These vulnerabilities allow an attacker with network access to the targeted system to cause DoS conditions or to gain an initial foothold on an operator's computer. If targeted operator has limited privileges, the attacker can exploit some of the flaws to gain full administrative access. CVE-2020-8477, a remote code execution issue affects the Information Manager component of System 800xA. The flaw, related to a component named ABBTracer, can be exploited remotely without authentication by convincing a user to visit a malicious website. Exploitation of the vulnerability can also result in the disruption of various functions. These flaws are caused by weak kernel object permissions, weak file permissions, and weak registry key permissions. These vulnerabilities impact various components, including OPC and MMS servers, application testing controllers, connectivity and communications components, batch management software, and information management software.

CVE-2020-8477, a remote code execution issue affects the Information Manager component of System 800xA.

Stuxnet-Style Vulnerability Found in Schneider Electric Software

Source: https://www.securityweek.com

A Stuxnet-Style vulnerability have been found in Schneider Electric Software. Stuxnet was designed to target Siemens'

A similar vulnerability, tracked as CVE-2020-7475, can be exploited to upload malicious code to Modicon M340 and M580 PLCs by replacing one of the DLL files associated with the software, could lead to process disruptions and other damage.

SIMATIC S7-300 and S7-400 programmable logic controllers (PLCs). The malware loads malicious code onto targeted PLCs by replacing a DLL file associated with the Siemens STEP7 controller programming software. A similar vulnerability, tracked as CVE-2020-7475, can be exploited to upload malicious code to Modicon M340 and M580 PLCs by replacing one of the DLL files associated with the software, could lead to process disruptions and other damage. The second flaw, tracked as CVE-2020-7489, is similar to CVE-2020-7475 with same CVSS score of 8.2. Schneider has released patches for both vulnerabilities, it is recommended user should apply these patches.

Security Misconfiguration: Server Version Discloser

Transport Sector, NCIIPC

Web Server is the one of the major components of any organisation that serves the services of the organisation to intended users. The attackers scan web servers to identify the type of server, its version number, and operating system details. The details are available in header fields and acquired through a HTTP request query to server commonly known as the web server banner. Current application development does not include security architectures by default. The application developer must implement security measures to avoid access to private or confidential resources. Improper server or web application configuration leading to various flaws like debugging enabled, incorrect folder permissions, using default accounts or passwords and setup/configuration pages enabled.

Security misconfiguration will occur due to failing to implement all the security controls for a server or web application.

Security misconfiguration vulnerability may be exploited if a network or application component is susceptible to attack due to an insecure configuration option. The web/application server can leak information from one or more "X-Powered-By" HTTP response headers. Access to such information allows the malicious user to identify other frameworks/components, web applications found integrated with and vulnerabilities of those elements may be exploited.

Impact: Attackers may try to gain unauthorized access or compromise the complete system by exploiting unpatched flaws or access default accounts, unused pages, unprotected files and directories, etc.

Symptoms: The applications might be vulnerable if they have the following:

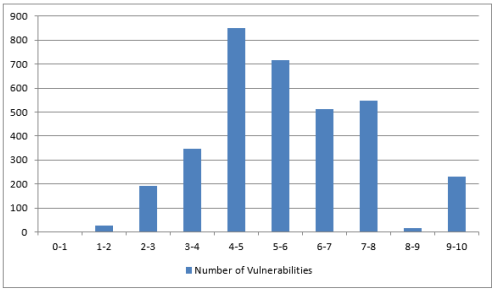
- Unnecessary features are enabled or installed (e.g. unnecessary ports, services, pages, accounts, or privileges).
- Enabling the default accounts and their passwords and unchanged.

- For upgraded systems, latest security features are disabled or not configured securely.
- The security settings in the application servers, application frameworks (e.g. Struts, Spring, ASP.NET), libraries, databases, etc. not set to secure values.
- The server does not send security headers or directives or they are not set to secure values.
- Usage of out of dated software

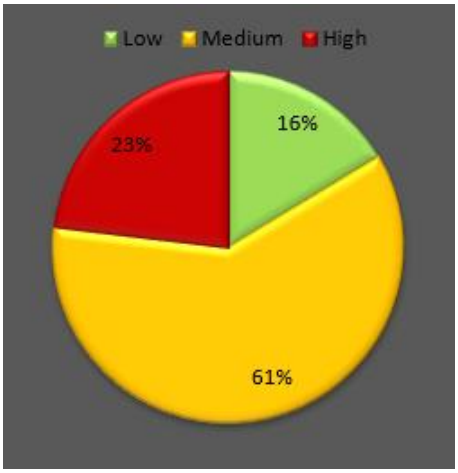
Quarterly Vulnerability Analysis Report

KMS Team, NCIIPC

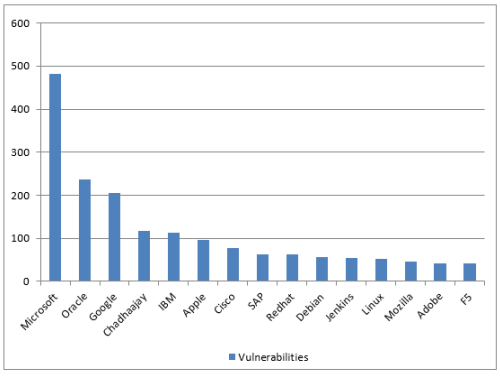
A total of 3436 vulnerabilities were observed from the month of Mar - May 2020. Most of the vulnerabilities had a score ranging from 4-7. 61 percent of total vulnerabilities reported were of medium severity. Microsoft, Oracle, Google, Chadhaajay and IBM were the top five vendors.



Severity	CVSS Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Mar	Apr	May		
Low	0-1	0	0	0	0	
	1-2	8	7	10	25	563
	2-3	56	74	62	192	
	3-4	153	122	71	346	
Medium	4-5	264	334	252	850	
	5-6	194	347	174	715	2078
	6-7	153	200	160	513	
High	7-8	202	208	139	549	
	8-9	6	5	5	16	795
	9-10	72	97	61	230	
Total		1108	1394	934		3436



S. No.	Vendor	No. of Vulnerabilities			Total
		Mar	Apr	May	
1.	Microsoft	173	164	145	482
2.	Oracle	0	231	5	236
3.	Google	81	54	71	206
4.	Chadhaajay	116	0	0	116
5.	IBM	25	32	55	112
6.	Apple	37	52	8	97
7.	Cisco	16	18	43	77
8.	SAP	16	28	19	63
9.	Redhat	22	19	21	62
10.	Debian	20	24	13	57
11.	Jenkins	36	9	9	54
12.	Linux	1	22	29	52
13.	Mozilla	23	10	13	46
14.	Adobe	42	0	0	42
15.	F5	7	30	5	42



Security App

Kaspersky to Remotely Support Weakly Connected PoS Devices

Source: https://www.darkreading.com/

This enables the solution to effectively protect ATMs, payment terminals and other similar devices in remote areas without affecting their productivity and service availability.

Kaspersky announces a new version of Kaspersky Embedded Systems Security that can now can remotely manage and update ATM and Point of Sale (PoS) devices located in areas with a 2G Internet connection. This enables the solution to effectively protect ATMs, payment terminals and other similar devices in remote areas without affecting their productivity and service availability. Also, Kaspersky Embedded Systems Security has been upgraded with a new Network Threat Protection component which prevents attacks on a network layer. The number of unique Kaspersky protected devices that encountered ATM/POS malware grew by nearly 2.5 times, according to statistics from Kaspersky Security Network. This suggests that ATMs, PoS and other similar systems are a tempting target for cybercriminals.

YARA 4.0.2 Released with Important New Features

Source: https://securityonline.info/

The latest major release of YARA includes new string modifiers, API changes, a reduced memory footprint, improvements to the PE and Cuckoo modules, and various bug fixes.

YARA 4.0.2 was released with some important new features and performance improvements. YARA is a highly popular open source tool designed to help researchers identify and classify malware samples. It has been described as "the pattern-matching swiss knife for malware researchers". The latest major release of YARA includes new string modifiers, API changes, a reduced memory footprint, improvements to the PE and Cuckoo modules, and various bug fixes.

Mobile Security

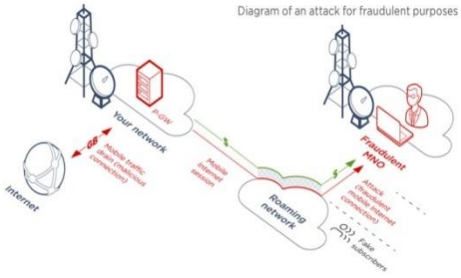
StrandHogg 2.0

Source: https://promon.co/

According to Google classified 'critical severity' (CVE-2020-0096), a successor of StrandHogg is found that doesn't abuse Android control setting 'TaskAffinity', attribute to an activity that leaves behind traceable markers. It executes through reflection i.e., by remaining hidden, the malicious app can assume the identity of a legitimate app. With its correct per-app tailored assets, it can dynamically attack any app on a given device simultaneously at the touch of a button, even on unrooted devices. It is much more difficult to detect than its predecessor, due to its code-based execution. StrandHogg 2.0 doesn't require any external configuration to execute and its attacks are obfuscated too. Once installed, it can trick the victim by showing a malicious version of an app when he/she clicks a legitimate app icon. This vulnerability works with older versions of Android, i.e., below 10.

Vulnerability in GTP and EPC Protocols

Source: https://thehackernews.com/



According to the report, Vulnerabilities in LTE and 5G Networks 2020, published by London-based cyber-security firm Positive Technologies, GPRS Tunneling Protocol (GTP) used by Mobile Network Operators (MNOs), which is responsible for data traffic over 2G, 3G and 4G networks, is vulnerable to data interception, impersonation, fraud and Denial of Service (DOS) attacks. Evolved Packet Core (EPC), the successor of GTP, which acts as the core network for wireless communications in 5G is also vulnerable to spoofing and disclosure attacks. The vulnerability lays in the fact that the subscribers' actual location is not checked by the protocol and so, it questions the legitimacy of the incoming traffic. The verification method of subscribers' credentials also poses a major architectural issue of this protocol. The firm suggests that whitelist-based IP filtering should be done at GTP level followed by analyzing traffic in real-time as per GSMA security recommendations which may block illegitimate activity.

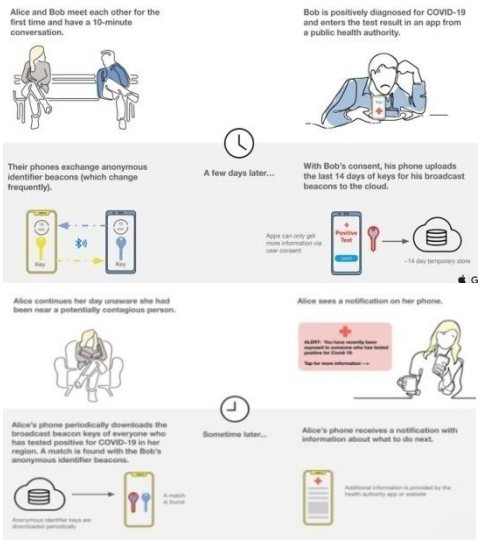
Misconfigured Firebase Exposes Android User Data

Source: https://www.comparitech.com/

Firebase is one of the most popular storage solutions provided by Google to store app data. Recently, a study by security research team at Comparitech has revealed that more than 24,000 apps are leaking user data due to misconfiguration of Firebase tool. Leaked user data includes email addresses, usernames, passwords, phone numbers, full name, chat messages, GPS data, IP addresses, street addresses, credit card numbers and photos of government-issued identification etc. A simple appending of ".json" to the end of a Firebase URL can expose this data to an attacker.

Contact-Tracing API by Apple and Google

Source: https://thehackernews.com/



Google and Apple have released a contact-tracing API to fight the ongoing COVID-19 pandemic. The API can be integrated into apps and it uses Bluetooth Low Energy Beacons (BLE) for contact tracing. This API has been released keeping in mind the privacy, transparency and consent of users and thus it doesn't use real-time location of app users. Whenever, two persons come in contact for more than 10 minutes, their phone exchanges anonymous identifier beacons. Later, if one of them is diagnosed as COVID-19 positive then by the consent of the infected person, the app will alert the users with whom the infected person has met in the last 14 days. This is done by uploading the infected person's beacon broadcast/ exchange data to a system. This helps the other users to decide whether

they should get tested or not. Singapore Government's TraceTogether app is already in line with this system of Apple and Google.

NCIIPC Initiatives

NCIIPC Building Resilience Against Cyber Attacks During COVID-19

Source: https://nciipc.gov.in/documents/NCIIPC_COVID19_Guidelines.pdf

The purpose of this document is to identify threat actors active during COVID-19 outbreak all over the world who are targeting Critical Information Infrastructure of India and to establish Safe and Secure Cyber Space. Various Threat vectors may include:

- Links to live tracking map and Mobile Apps
- Email attachments with malicious docs
- Donations for COVID-19
- IT fraud for credential harvesting (VISHING)
- Business Email Compromise / impersonation
- RDP and VPN credentials brute force
- SOHO Devices
- Invitation to fake VC/RAT application urls, etc.

Coronavirus related cyberattacks surge by 260% during lockdown, Kerala is the most targeted.

In order to prevent these, various guidelines were proposed for Management, IT/IS team and Remote Workers. Those guidelines are to Identify, Assess and carry out Risk Assessment of the organization/critical e-governance and service delivery functions of the Govt, which have to be operational during the lock down, focus on employee awareness training, apply application white listing, block unused ports, turn off unused services, monitor network traffic to prevent suspicious activities, apply least privilege controls to applications, security update/patches for all devices firmware/application, closely monitor privileged users, Configure Spoof Protection Controls, Validate Email Security Gateway Implementation, Block Macros in Microsoft Office Documents, Implement Strong Password Policies and so on.

Online Training Program by ISGF (India Smart Grid Forum) supported by NCIIPC

Source: https://indiasmartgrid.org/onlinetrainingprogram/img/csps.pdf

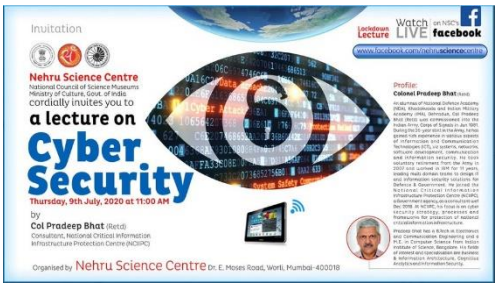
ISGF in collaboration with NCIIPC and VJTI conducted an online training program on Cyber Security for power systems from 21 May - 05 June 2020. It discussed about the role of NCIIPC in understanding Threats and Attacks on Smart Grid Cyber

Security for Power System and Cyber Security for Critical Infrastructure, basic Concepts of Cyber Security and Digital Grid, smart Grid Communications and Network Security, state of the Art Cyber Security Solutions, building Cyber Attack Resilience for Smart Grid Power Systems and Cyber Security Standards, audit and Assessment for Smart Utilities. A panel consisting of 12 expert tutors were available during this online training program including Gp. Capt. R.K. Singh (Director, NCIIPC), Sh. Abhijeet Raj Shrivastava (Sectoral Coordinator, NCIIPC) and Sh. Ganesh Kumar Sahu (Sectoral Coordinator, NCIIPC). The main objectives of the training were:

- To familiarize the Electric Utility Personnel on the importance of Cyber Security and associated risks
- To identify the Critical Information Infrastructure (CII) and the importance to protect CII from Cyber Threats.
- Understand state of the art cyber security solutions and practices followed by leading utilities in the world

According to an IT Governance Report, there were more than 1.7 billion data breaches and cyber-attacks in January 2019 alone

NCIIPC in NSC Mumbai Lockdown Lecture on Cyber Security



NCIIPC in collaboration with Nehru Science Centre (NSC) Mumbai organized a lockdown lecture on cyber security on Thursday, July 09, 2020 at Worli, Mumbai. Col. Pradeep Bhat (Retd), Consultant, NCIIPC delivered talk on usage of cyber space and cyber fraud. Cyber security plays an important role in our daily life mostly when we are making an online transaction.

NCIIPC Responsible Vulnerability Disclosure Program

Source: 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 Mar 2020 to May 2020 towards disclosure of vulnerabilities for protection of National Critical Information Infrastructure:

- Pankaj Kumar Varma
- Bindiya Sardhara
- Pankaj Kumar Thakur
- Shashwat
- Indrakant O Chaubey
- Kailas Patil

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

- Abdultaiyeb Chechatwala
- Navaneeth Shyam
- Omkar Amit Ghaisas
- Gourab Sadhukhan
- Numan Firfiry
- Krishnendu Samanta
- Md Anzaruddin
- Kishan Acharya
- Jerry Thomas

Upcoming Events - Global

July 2020

- ICS Lockdown, Virtual Conference 8-9 Jul
- ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Virtual 8-10 Jul
- CSO Summit Virtual Series, Virtual 23 Jul
- Threat Intelligence Summit, Virtual 23 Jul
- FutureConVirtual Eastern Conference, Virtual 28-30 Jul
- InfoSec Finance Connect 2020, Virtual 30-31 Jul

August 2020

- Black Hat USA, Virtual 1-6 Aug
- 29th USENIX Security Symposium, Virtual 12-14 Aug
- Charlotte 2020, Virtual Cyber Security Summit 13 Aug
- Artificial Intelligence Cybersecurity Conference, Virtual 18-20 Aug
- Philadelphia 2020, Virtual Cyber Security Summit 20 Aug
- ICS Cyber Security Conference 2020, London 31 Aug

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	

AUGUST 2020

S	M	T	W	T	F	S
30	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

September 2020

- Chicago 2020, Virtual Cyber Security Summit 1 Sep
- Gartner Security & Risk Management Summit, Tokyo 1-3 Sep
- 15th International Conference on Critical Information Infrastructures Security 2020, Bristol 2-3 Sep
- BillingtonCyberSecurity Summit, Virtual 8-9 Sep
- THOTCON, Chicago 11-12 Sep
- Global CISO Executive Summit, Marana 21-23 Sep
- Capital Region Virtual Cybersecurity Conference, Virtual 30 Sep

October 2020

- Cyber Security for Critical Assets (CS4CA) Europe, London 6-7 Oct
- Florida Cyber Conference, Orlando 8-9 Oct
- International Conference on Digital Forensics & Cyber Crime (ICDF2C), Cyberspace 15-16 Oct

SEPTEMBER 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			

OCTOBER 2020

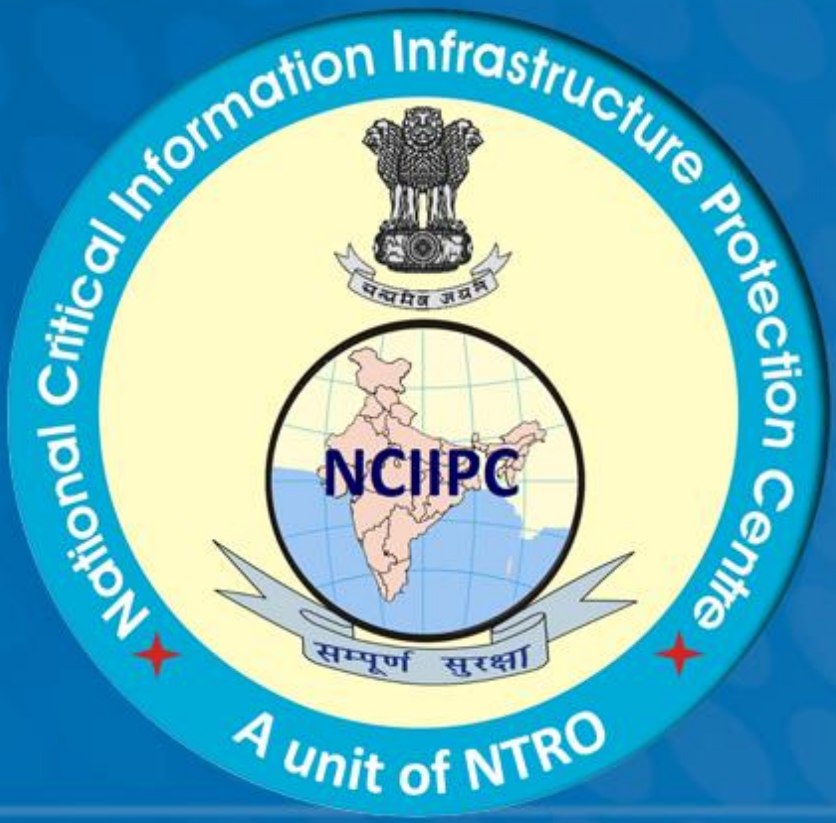
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

- Technology Leaders Club East Coast CISO Summit 2020, Boston — 18-20 Oct
- Virtual Cybersecurity and Fraud Summit, London — 20 Oct
- Nordic CISO Executive Summit, Stockholm — 21 Oct
- Gulf Information Security Expo and Conference (GISEC), Dubai — 26-28 Oct

Upcoming Events - India

- CISO MAG Summit & Awards INDIA 2020, Mumbai — 5 Aug
- Gartner Security & Risk Management Summit, Mumbai — 3-4 Sep
- cOcOn Hacking and Cyber Security Briefing Conference, Kochi — 16–19 Sep
- International Conference on Cyber security in Emerging Digital Era (ICCEDE 2020), Greater Noida — 9-10 Oct
- Virtual Cybersecurity Summit, Bengaluru — 26 Nov
- 21st International Conference on Cryptology in India (Indocrypt), Bengaluru — 13-16 Dec

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



Feedback/Contribution

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

Disclaimer

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