NEWSLETTER

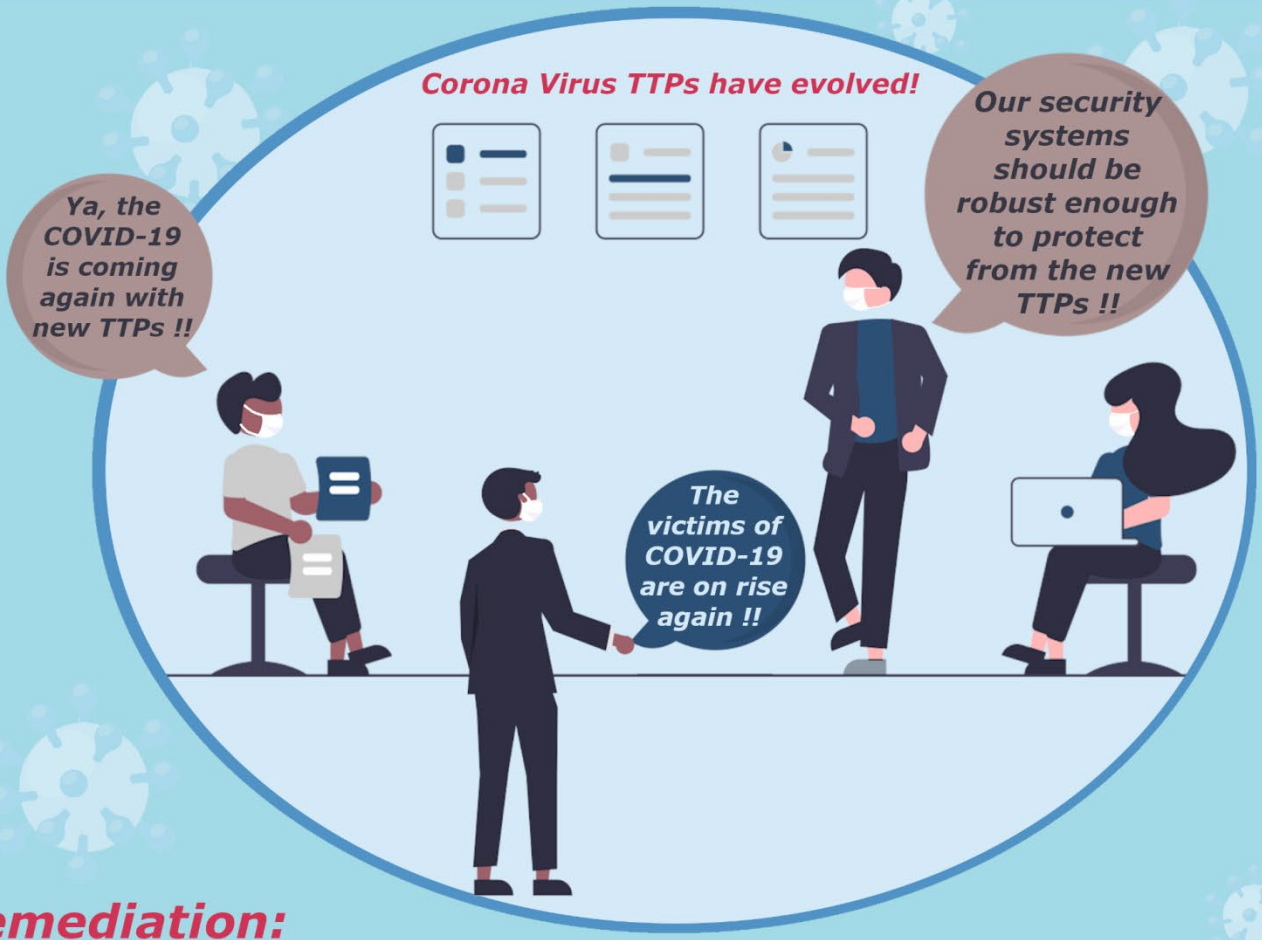
April 2021

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

#INDIAFIGHTSCORONA

सत्यमेव जयते



Remediation:

Wear Mask

Wash Hands Regularly

Maintain at Least 1 Metre Distance

Avoid Frequent Trips to the Market

If you have any symptoms like cough, fever or difficulty in breathing, avoid any kind of exposure and immediately call the helpline numbers (1075)

https://nciipc.gov.in
@NCIIPC
NCIIPC India
NCIIPC India
helpdesk1@nciipc.gov.in

VOLUME 5 ISSUE 2

@NCIIPC

NCIIPC Newsletter

April 2021

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

The first quarter of 2021, saw an increase in the coordinated cyber-attacks by alleged state actors linked groups targeting the Nation's Critical Sectors. The techniques have shifted from the conventional to a completely new set of innovative attack methodologies.

COVID-19 outbreak has resulted in a surge in targeting of Health Sector / Vaccine Research facilities with motive to steal research data, clinical trial data and IPRs. Automation of social engineering and phishing attacks are the new norm. NCIIPC has been pro-actively engaged with concerned organisations to share threat information and assist in remediation.

Government has initiated the process of developing a framework for maintaining the confidentiality and integrity of the supply chain including electronic components, necessary to build safe and resilient cyber ecosystem. In this framework, Government will draw out the list of equipment to be covered under the directive and the methodology to designate 'Trusted Products'.

International cooperation is the key to tackling the affliction of cyber threats. Taking down of Emotet Botnet infrastructure and DarkMarket, the world's largest illegal marketplace on the Dark Web trading in all kinds of drugs, counterfeit money, stolen credit card details, anonymous SIM cards and malware in an international operation involving coordinated cross-border and collaborative specialist operational analysis involving several countries is a case in point.

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

News Snippets - National

Implementation of Security Protocols to Protect Payments

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

The trade department has asked exporters to protect their payments from cyber fraud by implementing high secure protocols and follow better password practices in email communications as authorities cannot do much to reverse the transactions. In an advisory, it has been informed that bilateral trade disputes are increasing by email spoofing and phishing cyber frauds. In some cases, the victims who have supplied the goods end up being "neither have the goods in their possession nor have received the payment". Such types of problems can largely be resolved by implementing security protocols such as Domain Keys Identified Mail (DKIM), Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting and Conformance (DMARC). DKIM, SPF and DMARC are standard email signature protocols and all of these three prove that the sender is legitimate that their identity has not been compromised and that on behalf of someone else they are not sending email. It is required to follow better password policy on both the sender's and receiver's email IDs and exporters may confirm bank details by another secure channel such as a secure voice line to avoid cyber frauds completely.

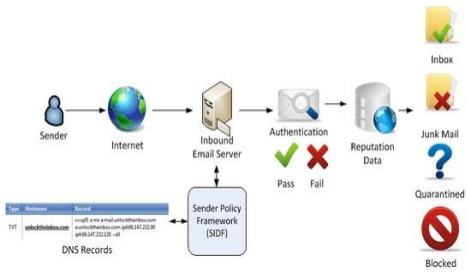


Image Source: https://blog.replyify.com/

DKIM, SPF and DMARC are standard email signature protocols and all of these three prove that the sender is legitimate that their identity has not been compromised and that on behalf of someone else they are not sending email.

India Approves a New Framework Against Cyber Threats

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

India has introduced its first and biggest framework to protect against data theft, vulnerabilities and other cyber-attacks threatening to national security. Maintaining the confidentiality and integrity of the supply chain including electronic components is necessary for ensuring security against malware infections. In view of these issues, a framework 'National Security Directive on Telecom Sector' has been recommended by NSA office, which will address 5G and supply chain concerns. In this framework, Government will declare a list of 'Trusted Sources/Trusted Products' for the benefit of the Telecom Service Providers (TSPs) in order to maintain integrity in supply chain and to discourage insecure equipment in the network. As per the directive, TSPs are required to connect only 'Trusted Products'. The National Cyber Security Coordinator (NCSC) will devise the list of equipment to be covered under the directive and the methodology to designate 'Trusted Products'.

India has introduced its first and biggest framework to protect itself against data theft, vulnerabilities and other cyber-attacks threatening to national security.

IT Minister Launches Tejas Tool and 'Work from Anywhere' Portal

Source: cio.economictimes.indiatimes.com, https://content.techgig.com

Image Source: https://media-exp1.licdn.com/

Sh. Ravi Shankar Prasad, Union IT and Communications Minister has launched a virtual intelligence tool Tejas and 'Work from Anywhere' portal at NICSI event on 28th January, 2021. Tejas is a virtual intelligence tool that will be useful to draw out critical information from data to make for policy decisions and improving efficiency in government services and citizen delivery. 'Work from anywhere' portal is a virtual environment which enables employee to access routine applications like mail, e-office, calendar and other departmental applications and communicate across through VC ensuring safety during Covid-19 pandemic with social distancing and work assurance from anywhere. 'e-Auction India' have also launched at the same event to cater to electronic forward and reverse auction requirements of the government organisations.

SEBI Mulls Cybersecurity Fusion Centre for Securities Market

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

Image source: https://www.teceze.com/

The process of setting up a cybersecurity fusion centre has been initiated by Market regulator Securities and Exchange Board of India (SEBI) to secure market infrastructure from cyber-attacks. Aim of this cybersecurity fusion centre or cyber lab is to detect cyber threats faster and resolve cyber-attacks efficiently and effectively. The cybersecurity preparedness or resilience of the entire securities market ecosystem would be strengthened by SEBI's three-tier structure. Division of technology and cybersecurity on SEBI to collaborate with the steering committee, operations centres and cyber security lab security at the respective Market Infrastructure Institutions (MIIs).

News Snippets - International

Cybersecurity: A Maritime Threat in 2021

Source: https://www.hstoday.us/, https://gmcg.global/

GMCG's (Global Maritime Consultants Group) Marine Cyber Security white paper, published on 24th December 2020, warns of increasing attacks which may originate via denial of service, phishing email, impersonation or various other ways and sets out measures that the maritime industry can take to protect against and prevent such attacks. An employee of ship operation could receive infected email which results in malware being downloaded and passed on through the systems associated with the ship. Most of these fraudulent emails are designed to make targets trigger malware installation on shore based or vessel IT networks and infect maritime supply chain or hand over sensitive information. The vulnerable areas are communication systems, cargo management systems, ship propulsion and power control systems, passenger services and the ship's bridge system. Ship owners need to have a recognised plan that identifies cybersecurity objectives to safeguard ship operation. A coalition of Maritime Organisations has recently updated a set of cybersecurity guidelines for the industry which includes general updates to best practices in the field of cyber risk management.

Image source: https://www.dnvgl.com/

> *The vulnerable areas are communication systems, cargo management systems, ship propulsion and power control systems, passenger services and the ship's bridge system.*

Authorities Take Down World's Largest Darkweb Marketplace

Source: https://thehackernews.com/

DarkMarket, the world's largest black marketplace for illicit goods on the dark web, has been shut down as a result of an international operation conducted by law enforcement from Germany, Denmark, United Kingdom (The National Crime Agency), Australia, Moldova, Ukraine and USA (DEA, FBI, and IRS) with support of the Europol. The Darkmarket was an important point of aggregation for online cybercriminals that traded all kinds of drugs, stolen or counterfeit credit card details, counterfeit money, anonymous SIM cards and off-the-shelf malware. The criminal infrastructure, including more than 20 servers in Moldova and Ukraine that were used to conduct the operations has been taken offline. At the time of closure, DarkMarket is believed to have almost 500,000 users and more than 2,400 sellers with over 320,000 transactions resulting in more than 4,650 bitcoin and 12,800 monero transferred. The overall transactions correspond to a sum of more than 170 million dollar. A 34-year-old Australian national who is alleged to be the mastermind behind DarkMarket has been arrested by operation led by Police in city of Oldenburg, Germany. The investigation is still going on, investigators may get new leads by examining obtained data as

Image source: https://www.europol.europa.eu/

> *The criminal infrastructure, including more than 20 servers in Moldova and Ukraine that were used to conduct the operations has been taken offline.*

a result of the operation to further investigate moderators, sellers and buyers involved in activity of the marketplace.

Image source: https://purplesec.us

Threat actor could convince employee to log into the fake VPN page operated by the cyber criminals and perform reconnaissance to locate someone with higher privileges who could perform username and e-mail changes using captured credentials.

FBI Warns of Employee Credential Phishing via Phone, Chat

Source: www.securityweek.com/, image.communications.cyber.nj.gov/

A Private Industry Notification (PIN) has been issued by Federal Bureau of Investigation to warn of attacks targeting enterprises, in which threat actors attempt to obtain employee credentials through vishing (voice phishing) using VoIP platforms or chat rooms. Cyber-criminals are taking advantage of Covid-19 pandemic to exploit possible misconfiguration and lack of monitoring for remote network access and user privileges. According to FBI case information, employees were tricked to log into a phishing webpage during the phone calls in order to capture the employee's username and password that allow cyber criminals ability to escalate privileges of the compromised employees' accounts and gain further access into the network often causing significant financial loss. Threat actor could convince employee to log into the fake VPN page operated by the cyber criminals and perform reconnaissance to locate someone with higher privileges who could perform username and e-mail changes using captured credentials. It is recommended to implement multi-factor authentication (MFA) for employee accounts, actively monitor the environment for unauthorized access or modifications, adopt the least privilege principle (especially for new employee accounts), employ segmentation of network and issue two accounts for admins- one for email and another for making changes to systems.

Image source: https://i1.ytimg.com/

Sophisticated AI models are used in DeepArmor to analyse thousands of characteristics of payloads in memory or permanent storage.

Artificial Intelligence to Counter Cybersecurity Threats for Drones

Source: https://www.aviationtoday.com/

In a press release on 19th Jan 2021, SparkCognition and SkyGrid announced a new collaboration to deploy AI-powered cybersecurity directly on drones, protecting them from zero-day attacks during flight. Traditional signatures based technology of known threats to detect malicious actors won't be adequate to detect never-before-seen attacks. Intelligent AI based approach would detect and prevent cyberattacks from impacting a drone, a payload or a ground station more accurately. According to the release, SparkCognition's DeepArmor integrated with SkyGrid's airspace management system, AeriosOS, will be installed directly on drone hardware to function even without network connectivity. Sophisticated AI models are used in DeepArmor to analyse thousands of characteristics of payloads in memory or permanent storage. As a result, it does not need prior knowledge of a specific threat to make a classification and has been very

successful at catching advanced zero-day threats. When deployed on drones, all payloads will be autonomously monitored, intercepted, encrypted, automatically quarantined and moved to a secure location where it cannot run but is available for post-flight forensics by DeepArmor.

World's Most Dangerous Malware Emotet Disrupted

Source: https://www.hstoday.us/

Emotet, one of the most significant botnets of the past decade has been disrupted in a collaborative operation by Law enforcement and judicial authorities in Germany, Netherlands, United States, United Kingdom, Canada, France, Lithuania and Ukraine coordinated by Europol and Eurojust. Emotet malware was delivered via phishing email containing either as a malicious word document or link within the email through a fully automated process. Users could be prompted to "enable macros" by opening these documents or clicking on the link provided so that hidden malicious code could run and install Emotet malware on a victim's computer. Started as a banking trojan, the malware has evolved into one of the most aggressive platforms for spreading other types of malware to perform cyberattacks like ransomware over the years. A combination of both updated cybersecurity tools like operating systems and antivirus, and cybersecurity awareness is essential to avoid falling victim to sophisticated botnets like Emotet. Users need to carefully check their email and avoid opening messages and especially attachments from unknown senders.

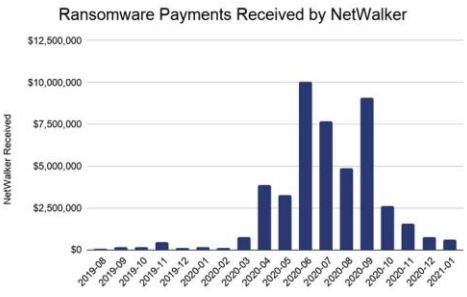
Image source: krebsonsecurity.com

> *Users could be prompted to "enable macros" by opening these documents or clicking on the link provided so that hidden malicious code could run and install Emotet malware on a victim's computer.*

Arrest, Seizures Tied to Netwalker Ransomware

Source: https://krebsonsecurity.com/, https://thehackernews.com/

The dark website used by the NetWalker ransomware cybercrime group to publish data stolen from its victims has been seized by U.S. and Bulgarian authorities as part of a coordinated law enforcement action. NetWalker is a ransomware-as-a-service product which emerged as a popular choice of ransomware strain besides Maze, Ryuk, Doppelpaymer and Sodinokibi with numerous hospitals, schools, companies, municipalities and universities targeted by the cybercriminals to extort victims. As part of double extortion, The NetWalker operators steal data before encrypting the files and threaten to publish the information if the target refuses to pay the ransom. According to report, at least 305 victims from 27 countries have been targeted by NetWalker.



All equipment and services remotely linked to Chinese companies should be considered a cyber-security and business risk, the agency said.

DHS Warns of Data Theft Risk when using Chinese Products

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

The U.S. Department of Homeland Security (DHS) has warned U.S. companies against using hardware equipment and digital services created or linked to Chinese companies. The DHS has suspected that Chinese products could contain backdoors or any other hidden data collection mechanisms that could be used by Chinese authorities to collect data from western companies and forward the information to local competitors to further China's economic goals thereby causing damage to other countries. All equipment and services remotely linked to Chinese companies should be considered a cyber-security and business risk, the agency said. The DHS has recommended U.S. businesses to implement appropriate cybersecurity measures that could help as part of a multi-layered data security policy.

It is also revealed that the group had targeted more than 80 Israeli firms.

Iranian Hackers Hit Top Israeli Defence Contractor

Source: https://www.haaretz.com/

Israel's state-owned Israel Aerospace Industries (IAI) has been hacked by the hacking group Pay2Key linked to Iran. In a tweet and update to their website on darknet, it is seemingly indicating that they had managed to enter the IAI's internal system, which sits on the ELTA.co.il domain and may have access to sensitive information. It is also revealed that the group had targeted more than 80 Israeli firms. Israeli cybersecurity firms first discovered this hacker group in November. This group mainly focuses on ransomware attacks. The details of about 1,000 users from the defence contractor's internal system have also been posted but no ransom is demanded. The hack may have taken place in the past and hackers may not currently have access to the system.

The operation named as "Operation Nova" was coordinated by Europol officials and led by officers from the German Reutlingen Police Headquarters.

Safe-Inet, Insorg VPN Services Shut Down by Law Enforcement

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

The infrastructure supporting Safe-Inet and Insorg VPN and proxy services known for providing safe haven to cybercriminals for attacks their victims has been seized in a cooperative operation by Law enforcement agencies from US, France, Germany, Switzerland and the Netherlands. The operation named as "Operation Nova" was coordinated by Europol officials and led by officers from the German Reutlingen Police Headquarters. Three services (insorg.org, safe-inet.com and safe-inet.net) have been described as "bulletproof hosting services" by Law enforcement. The services have been active for more than a decade and often used to mask the real identities of ransomware gangs, online phishers, web skimmer (Magecart) groups and

hackers involved in account takeovers allowing them to operate from multiple layers of anonymity and stable connections. The services used were charged between $1.3 per day to $190 per year and provided up to 5 layers of anonymous VPN connections.

China-linked TA413 Group Target Tibetan Organisations

Source: https://securityaffairs.co/

Tibetan organisations across the world have been targeted by Chinese cyberespionage group TA413 using "FriarFox", a malicious Firefox add-on. Successful installation of FriarFox add-on, allowed threat actor to steal Gmail and Firefox browser data and deliver malware on infected systems. The attack chain begins with spear-phishing email messages that attempt to trick victims into visiting websites which eventually asked them to install a Flash update in order to view the site's content. Security researchers found that the websites were set up to serve the malicious add-on only to Firefox users with an active Gmail session. The victims are served the FriarFox extension from hxxps://you-tube[.]tv/download.php, then they are prompted to allow the download of software from the site, and they are prompted to "Add" the browser extension named "Flash update components" by approving permissions of the extension. The browser redirects to the dangerous webpage hxxps://Tibet[.]net and it is displayed the message "Flash update components has been added to Firefox". The FriarFox add-on also contacts the C2 server to retrieve the PHP and JS-based payload Scanbox frameworks which has been used by multiple APT groups to carry out watering hole attacks.

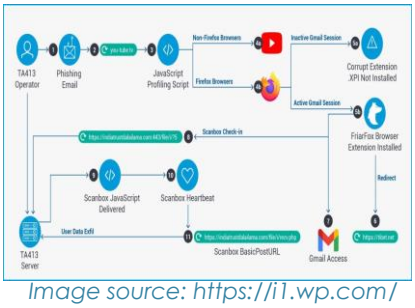


Image source: https://i1.wp.com/

The FriarFox add-on also contacts the C2 server to retrieve the PHP and JS-based payload Scanbox frameworks which has been used by multiple APT groups to carry out watering hole attacks.

Trends

AIR-FI Attack Turns RAM in Air-Gapped Systems into WiFi

Source: https://latesthackingnews.com/

Researchers from Ben-Gurion University of the Negev, Israel, have discovered an interesting attack strategy that targets air-gapped systems named AIR-FI. This attack aims transforming the RAM of air-gapped systems into WiFi. The attack method exploits the capability of air-gapped systems to generate electromagnetic waves as the current flows through them. This method infects the targeted air-gapped system with a malware that command the RAM to generate waves with frequencies consistent with the usual WiFi spectrum. A receiving WiFi capable device, in this way, could catch the data from air-gapped systems as it receives that WiFi. Once done, the attacker is then capable to infect a nearby WiFi

The attack method exploits the capability of air-gapped systems to generate electromagnetic waves as the current flows through them.

device to receive the leaked data. After successful infection, the malware would then steal data from the air-gapped system, leak it to the air as WiFi for the receiving device.

Image source: https://thehealthcaretechnologyrepo

A group called "UnwPock" has been active since June 2020 and is targeting medical devices and pharma companies, global vaccine approval authorities and hospitals in India.

Healthcare Organisations Targeted to Leverage Covid-19 Data

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

It has been observed that currently hospitals and healthcare organisations are the most affected among other sectors in cyberattacks world-wide. Cyfirma, a Singapore-based security research firm said that cyber-attack campaigns originating from Russia, China, Korea, and Middle East have been targeting pharmaceutical companies in India to steal COVID-19 vaccine research data, supply chain and vaccine production information, patient information, clinical trials data. Organisations in 12 other countries are also being targeted apart from India. A group called "UnwPock" has been active since June 2020 and is targeting medical devices and pharma companies, global vaccine approval authorities and hospitals in India. Another campaign called "cold unseco33" has also been attacking global pharma companies including those in India working on COVID-19 vaccines. Multi-stage ransomware attacks are the most common among other cyberattacks by cyber criminals to exfiltrate intellectual property, sensitive databases and customer information. The attacker threatens to disclose the breached data publicly unless the ransom is paid within the designated time limit. A report said that in New Delhi monthly cyberattacks per healthcare organisation jumped to 37% in 2020 in last 12 months.

Security Flaw leading to Cross-layer and DNS Poisoning Attacks

Source: https://cyware.com/

A new attack technique called cross-layer attack has been identified, which combines vulnerabilities across multiple network protocol layers to attack the target system. The cross-layer attack is possible because a flaw in Pseudo-Random Number Generator (PRNG) allows an attacker to obtain the internal state of any application using that PRNG. After the internal state of the PRNG from one of the Open Systems Interconnection (OSI) layers has been obtained, this security flaw makes it possible to use the obtained information to estimate the random number value in other OSI layers as well. Estimating the PRNG value allows attackers to carry out DNS cache poisoning attacks to target Linux systems locally and remotely. The security flaw can allow hackers to recognise and track Android-based and Linux-based devices. The cross-layer attack works even when the browser privacy mode is On or VPN is in use. To fix this flaw a patch has been developed based on a stronger PRNG using SipHash.

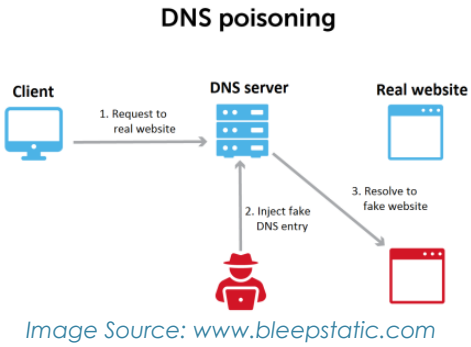


Image Source: www.bleepstatic.com

FBI warns Hijacking of Home Security Devices for 'Swatting'

Source: https://www.ic3.gov/Media/Y2020/PSA201229

The Federal Bureau of Investigation (FBI) has issued a warning to users of smart home devices with voice and cameras capabilities to use unique, complex passwords and enable 2 Factor Auntentication to help protect against "swatting" attacks. Swatting is a dangerous prank where police are called to a home with a fake emergency. Recently, smart home device manufacturers have notified law enforcement that offenders have been using stolen e-mail passwords to access smart devices, including video and audio capable home surveillance devices, to carry out swatting attacks. The offenders are taking advantage of customers who re-use their email passwords for their smart devices. The attackers use stolen email passwords to log into the smart device and hijack features, including the live-stream camera and device speakers. Then they call emergency services to report a crime at the victims' residence. As law enforcement responds to the residence, the attackers watch the live stream footage and engages with the responding police through the camera and speakers. In some cases, the attacker live stream the incident on shared online community platforms.

Image Source: https://assets.change.org/

The offenders are taking advantage of customers who re-use their email passwords for their smart devices.

Homomorphic Encryption: The 'Golden Age' of Cryptography

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

The homomorphic encryption technology uses lattice-based algorithms to hide the input, intermediate values, output, and even the function being computed from anyone not holding the secret decryption key. In other words, this technology allows computations to be performed on encrypted data. Homomorphic encryption makes it possible to submit sensitive financial data and prove that it meets requirements or is in compliance without ever displaying the underlying data. Homomorphic encryption when combined with blockchain could usher in new types of smart working agreements, contracts, and apportion settlements that aren't possible today. It allows members of a blockchain to share data in more secure and flexible ways. Homomorphic encryption also supports next-gen cybersecurity functionality makes it possible to develop software free of bugs and security flaws without revealing proprietary code. Homomorphic encryption also allows the owner of data to gain far greater and granular control over it. This technology is particularly suited to big data environments, where it's necessary to tap enormous cloud computing power and keep the underlying data private.

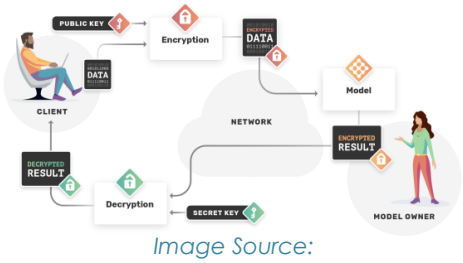
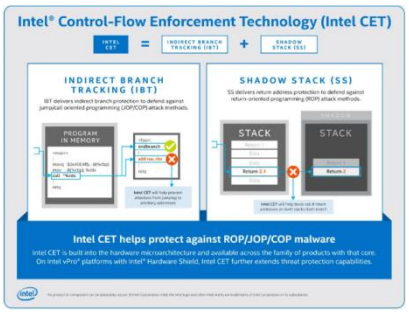


Image Source: https://blog.openmined.org/

Homomorphic encryption also supports next-gen cybersecurity functionality makes it possible to develop software free of bugs and security flaws without revealing proprietary code.

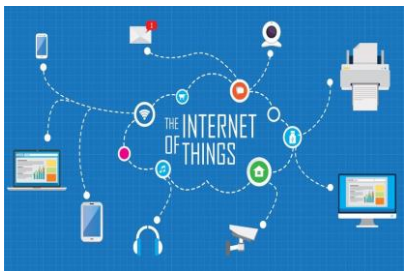


Intel CET blocks these JOP and ROP attempts by triggering exceptions when the natural flow of a program is modified.

Intel Security Feature for Chromium Browsers

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

Chromium-based browsers such as Google Edge and Microsoft Edge will soon support the Intel Control-flow Enforcement Technology (CET) security feature to prevent a wide range of vulnerabilities. Intel's CET is a hardware security feature designed to protect programs from Jump Oriented Programming (JOP) and Return Oriented Programming (ROP) attacks that modify an application's normal flow so that an attacker's malicious code is executed instead. Intel CET blocks these JOP and ROP attempts by triggering exceptions when the natural flow of a program is modified. These vulnerabilities include attacks that perform remote code execution or bypass a browser's sandbox while visiting web sites. Through an implementation called Hardware-enforced Stack Protection Intel CET is supported by Windows 10. To support this feature Windows applications must first be compiled with the /CETCOMPAT linker flag in Visual Studio. After this flag is compiled, a program will be marked as CET Shadow Stack-compatible and opted into the security protection.



IoT devices are easy target by the cyber-criminals because the IoT device industry is very convenient for business. Everyday many IoT devices are created that are Wi-Fi compatible and one can easily control them using smartphone.

IoT: The New Era of Technology

Threat Assessment Team, NCIIPC

The Internet of Things (IoT) is a network of devices that are embedded with various softwares, sensors and other technologies for connecting and exchanging data with other devices and systems on the Internet. IoT devices are now embedded in every part of our lives, with the continuous growth of devices on internet each day threats to the IoT devices are also increasing, especially in the areas of privacy and security. IoT devices are easy target by the cyber-criminals because the IoT device industry is very convenient for business. Everyday many IoT devices are created that are Wi-Fi compatible and one can easily control them using smartphone. Below mentioned are the main threats to IoT devices:

- Botnet: Targeting IoT devices by using malware for creating an IoT Botnet is big business. With the large number potentially vulnerable devices connected to the internet, a Botnet consisting of IoT devices will be much larger than a Botnet of compromised computers used by the cyber-criminals for cyber-crime activities.
- Crypto-miners: With crypto-miners targeting IoT devices to mine cryptocurrencies seems like an easy plan to execute, but most IoT devices lack the hardware required to mine cryptocurrencies. Botnet such as 'LiquorBot', 'Mirai-variant' and 'Linux.MulDrop.14' have all tried mining cryptocurrencies.
- Ransomware attacks: IoT devices are now targeted by ransomware attacks because for a threat actor targeting an

IoT device could open path to compromise many other devices rather than focusing on a single device for ransom.

- Denial of Service: Denial-of-service (DoS) attacks can also occur in an IoT device by the cybercriminals, by Flooding networks with requests choke their resources and to make them offline. DoS attacks can disable all the functionality and services of an IoT device which are assigned to its actual users.

Denial-of-service (DoS) attacks can also occur in an IoT device by the cybercriminals, by Flooding networks with requests choke their resources and to make them offline.

Following are the preventive measure for securing IoT devices from these attacks:

- Connect IoT devices using secure Wi-Fi.
- Encrypt computer connection using a virtual private network (VPN).
- Restrict physical access to IoT devices.
- Keep all IoT device software up-to-date.
- Change defaults and use strong passwords.

References:

[1] https://blog.nettitude.com/iot-cybersecurity-threats-how-cybercriminals-target-iot-nettitude

[2] https://wire19.com/warning-iot-devices-at-risk/

[3] https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-quarterly-threats-mar-2017-1.pdf

Emerging Cyber Threat Predictions in 2021

BFSI Sector, NCIIPC

After the worst pandemic of century, what the New Year 2021 will bring in cyber world? Here are some security industry forecasts, trends, themes and cyber security predictions.

- Increased Artificial Intelligence in attacks: Hackers are expected to inject malicious code to manipulate algorithm activities, such as crypto-mining malware that could turn machines into attack systems. Attacks will become more complicated with the rise of 5G, and quantum computing.
- Deepfake attacks to increase: In coming times, deep fake technology will be more widely used to cause misinformation and corporate espionage. The technology will influence perception and trick victims into taking unintended actions, similar to social engineering attacks, but could be much more insidious.
- Increase in impersonating IT systems: Attackers could use virtualisation techniques to create replica or illusory system environments. For example, hackers will be able to create a look alike ERP within an Intranet to trick unsuspecting users into divulging classified information or to collect data for future malicious activities.

In coming times, deep fake technology will be more widely used to cause misinformation and corporate espionage.

- Increased Supply Chains attacks: As supply chains get more connected, complex, and goods and services flow through more digital systems, a compromise might have a major impact. There will be more growth in supply chain attacks by state actors. Attackers could repeat attack methods use in the case of the SolarWinds hack in future.
- Edge devices will be a target: When computing power and data is spread across a broad footprint, digital risk associated with perimeter defence, passwords and authentication, data storage, protection, back-up etc. will present more challenges to cyber security people. Businesses need to improve cyber security best practices to include the mitigating risk that comes with the adoption of edge computing.
- Multimorphism on the rise: 'Multi-morphic' malware will be a reality. 'Multi-morphic' malware can switch seamlessly across stages of a cyber-attack and deciphering the actual behavioural path of such malware can be difficult. It is very difficult to identify these types of malware because of no historical evidence.
- Covid-19 related phishing scams will continue: Phishing campaigns related to Covid-19 and associated scams spoofing offers of healthcare payments, government-sponsored relief loans, or vaccine dissemination will continue.
- Advanced Persistent Threats (APT) attacks sponsored by state actors likely to be higher side.
- The darkweb will allow criminals to buy access into more sensitive corporate networks.
- Mobile devices, including smartphones, will be attacked in latest ways, including app stores.
- Identity and multi-factor authentication (MFA) will take centre stage as passwords start to go away in a tipping-point year.

'Multi-morphic' malware can switch seamlessly across stages of a cyber attack and deciphering the actual behavioural path of such malware can be difficult.

The darkweb will allow criminals to buy access into more sensitive corporate networks.

References:

[1] https://ciso.economictimes.indiatimes.com/news/emerging-cyber-threat-predictions-in-2021/80384112/

[2] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-21-security-predictions-for-2021.html

Evolution of Botnets

Director, NSAC, NCIIPC

Ever evolving Cyber intrusions/threats are giving nightmares to information security teams of all organisations in different sectors and geographical locations across the nations. With passage of time, as the defence mechanisms of networks evolve to identify and thwart threats, malicious attackers/hackers are devising new ways to bypass the detection mechanisms and build more resilient CnC (Command and Control) networks. Bot or Zombie is a

terminology that is primarily used for compromised controllable machines that receive and execute commands from BotMasters through CnC. A collection of such Bots is termed as Botnet, which over the time has evolved to become resilient and stealthy. A Botnet broadly passes through the following lifecycle:

- Spreading of infection by an evolving Bot army.
- Maintaining upstream/downstream communication between Bots
- Execution of commands at the behest of Bot Master through CnC servers.
- Uploading stolen data dump (if any) to a staging server.
- Indicative reasons for the rampant growth in Botnets are:
- Blocking of thousands of ever evolving bots is practically difficult to achieve by any Network Defender.
- Traffic originated from Bots anonymize the identity of actual CnC.
- Used for DDOS/Spam mails.
- Use in cyber-criminal activities.
- Very high volume of exploitation is possible.

Bot or Zombie is a terminology that is primarily used for compromised controllable machines that receive and execute commands from BotMasters through CnC.

Botnet Types: Botnets have gone through a transformation in terms of resiliency, stealth and anonymity as highlighted in figure 1.

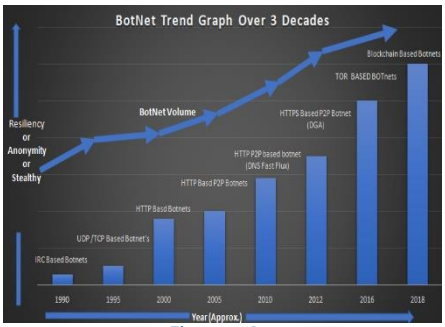


Figure: 1

- IRC based Botnets belong to the first generation, where Bots receive commands through IRC chatrooms from hardcoded CnC servers. However, IRC traffic can be easily distinguished by network defenders, thus making these Botnets identifiable and blocked.
- Within a decade after advent of HTTP based Botnets, downstream (commands) and upstream data (dump) started happening over HTTP channels only. Complexity of identification of HTTP based Botnets increased as most of the network's defences allow ingress/ egress of HTTP traffic. However, mature SIEMs are capable of identifying the same with help of machine learning.
- Decentralisation transition occurred with P2P (Peer to Peer) Botnets, which distributed the centralised authority to decentralized servers eradicating the weakness of Single Point of Failure (SPOF) in earlier Botnets.
- Another evolution in decentralised P2P Botnets mentioned above happened in terms of evading detection techniques, thus making it difficult for network defenders to track the botnets. Following methodologies are used:
  - DGA algorithm.
  - DNS Fast Flux.
- Anonymity of botnets scaled up tremendously with advent of Tor based botnets. For anonymity these botnets also use VPNs as an alternate communication channel.
- Latest evolution of sophisticated botnets is blockchain based botnets. These blockchain based botnets are difficult to

Decentralisation transition occurred with P2P (Peer to Peer) Botnets, which distributed the centralised authority to decentralized servers eradicating the weakness of Single Point of Failure (SPOF) in earlier Botnets.

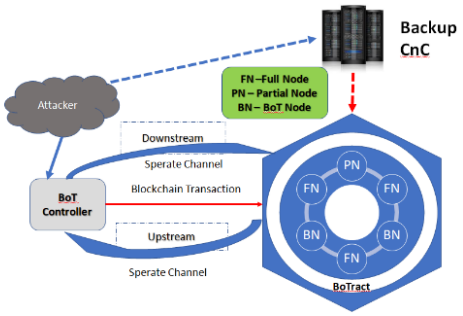


Figure: 2

identify and block because of legitimisation and acceptability of blockchain technology that powers crypto currencies across the world.

- Blockchain based Botnets: Blockchain based botnets rely on blockchain smart contracts, termed as Botract, to control botnets. The blockchain based botnets, clubbed with P2P, VPN and ToR, provide an exceedingly high degree of stealth, anonymity and resilience. However, resilience of blockchain botnets also depends upon the amount of ETH (Etherium) or BTC (Bitcoin) that has to be being spent for each transaction. Data transactions in blockchain based botnets happens in three stages, as mentioned in figure-2:
  - Downstream data which are usually commands to be executed by the bots.
  - Upstream data which is data collected from victim servers. This upstream also confirms to the botmaster about the active bots available for use.
  - Backup CnC server IP transactional details to avoid seizure of the same.

Trends show that attackers are opting for backup server transactions for adding resiliency to botnet CnCs with lower cost implications.

Maintaining all the streams of data with almost 10,000 bots spread globally has a very high cost in terms of ETH or BTC, which may not be a sustainable solution. Trends show that attackers are opting for backup server transactions for adding resiliency to botnet CnCs with lower cost implications. Separate channels for upstream and downstream data are maintained in the backup CnC servers to reduce the transactional details in Blockchain ledgers.

Conclusion: With usage of new technologies to create botnets, detection and blocking of the same is becoming a challenging task for network defenders. Blockchain technology is resistant to censorship, because blocking of the same may hamper genuine users, who are associated with legalised usage of crypto currencies. These blockchain based botnets also add to the decentralisation of the command and control of the network. Blockchain transaction ledgers are publicly available, which may reveal the botnet details. However, use of ToR and VPNs add stealth to botnet traffic, enabling them to bypass the detection techniques. Fully automated blockchain dependent botnets have not been seen till date as they are very expensive to sustain. However, blockchain botnets with downstream command or backup as CnC have already been demonstrated due to their lower cost implications. Network defenders will certainly have to evolve their detection methodologies for defending their networks.

Blockchain technology is resistant to censorship, because blocking of the same may hamper genuine users, who are associated with legalised usage of crypto currencies.

References:

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

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

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

[4] https://resources.infosecinstitute.com

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

[6] https://internetpolicy.mit.edu

[7] Assessing the threats of Blockchain based BoTNets by Leon Block, Nikolaos Alexopoulos, Emine Saracoglu, Max Muhlhauser and Emmanouil Vasilomanolakis

[8] The zombie roundup: understanding, detecting and disrupting botnets by Evan Cooke, Farnam Jahanian, Danny McPherson

Intel's new vPro Processors aim to defend against Ransomware

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

Ransomware protection will be implemented in Intel's new 11th Gen Core vPro mobile processors with the goal of strengthening security and visibility at the hardware level without disrupting the user experience. The number and complexity of ransomware attacks are growing as operators find new ways to evade detection. Many ransomware strains have evolved to bypass behavioural-based and traditional signature-based detection techniques. Some new variants are using virtual machines to hide behind to avoid antivirus software. Many threat actors have adopted the dual-extortion technique in which they stole information before encrypting and then threaten victim to disclose the breached data publicly unless the ransom is paid within the designated time limit. Intel's Threat Detection Technology (TDT) feature included in Intel Hardware Shield will detect ransomware and other security threats. Machine learning capabilities has been implemented in Intel's TDT to detect attacks in real time without causing lags in the user experience.

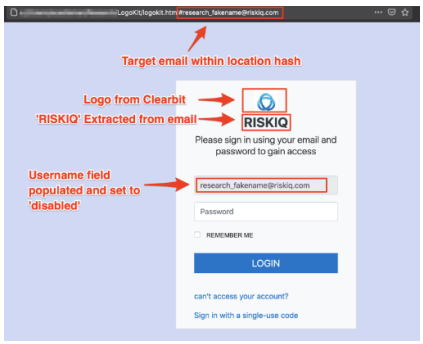
Image source: https://www.gamersrd.com/

Intel's Threat Detection Technology (TDT) feature included in Intel Hardware Shield will detect ransomware and other security threats.

New Cybercrime Tool can build Phishing Pages in Real-time

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

A novel phishing toolkit named as "LogoKit" has been developed by a cybercrime group that could change logos and text on a phishing page in real-time to adapt to targeted victims. According to threat intelligence firm RiskIQ, LogoKit has already been deployed in the wild and fetches the company logo from a third-party service, such as Clearbit or Google's favicon database, once a victim navigates to the URL. LogoKit has been used from services ranging from generic login portals to false SharePoint portals, Adobe Document Cloud, Office 365, OneDrive and



Most of these services are whitelisted inside corporate environments and prompt little alerts when loaded inside an employee's browser.

several cryptocurrency exchanges to mimic and create login pages. It performs an AJAX request to send the email and password entered by victim to an external source, and finally, redirecting the user to legitimate corporate web site. Since LogoKit is a collection of JavaScript files, public trusted services like Firebase, Oracle Cloud, GitHub, and others can also host its resources. Most of these services are whitelisted inside corporate environments and prompt little alerts when loaded inside an employee's browser.

Microsoft will alert Office 365 Admins of Forms Phishing Attempts

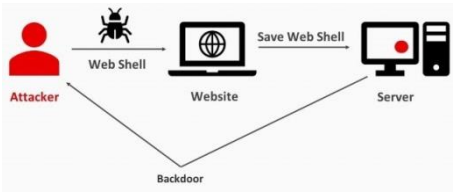
Source: https://www.bleepingcomputer.com/

Image source: https://www.metacompliance.com

Microsoft has previously added Microsoft Forms proactive phishing detection feature to improve security of the product by blocking phishing attempts from abusing surveys and forms created using the app. Now, Microsoft is planning to add new security warning feature to default alert policies of the Security and Compliance Centre (SCC) to inform admins of detected phishing attempts. Microsoft Forms enables mobile and web users to create surveys, quizzes and polls for collecting feedback and data online. Malicious password collection in forms and surveys will be detected proactively using automated machine review by the phishing protection feature and it will block phishers from abusing Microsoft Forms to create phishing landing pages. Admins get alerts of any users or forms blocked in their tenants for potential phishing. Microsoft is now working on also including these phishing activity alerts to SCC's alert centre. Office 365 admins could review and unblock the users if they consider that no malicious intent was behind their data collection attempts once the notifications are added to the message centre.

Microsoft warns of an increasing number of Web Shell Attacks

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



Web Shell Backdoor

According to Microsoft report the number of monthly web shell attacks has increased by almost two times since last year with an average of 140,000 such malicious tools being found on compromised servers every month. Web shells are scripts or tools that are deployed on hacked servers to gain and/or maintain access, to remotely execute arbitrary commands or code to deliver additional malicious payloads. The list of preventive measures that should be taken to avoid web shell attacks include:

- Web applications and web servers should configure properly and latest security patches should be deployed
- Utilize the Windows Defender Firewall, network firewall and intrusion prevention devices to prevent command-and-control (C2) server communication among endpoints whenever

possible
- Enable antivirus protection on web servers
- Logs from web servers should review frequently

The U.S. National Security Agency (NSA) has also warned about web shell attacks on vulnerable web servers. The NSA has a dedicated GitHub repository with tools that can be used by admins and organisations to detect and block web shell threats. The repository includes Scripts for "Known-Good" file comparison, Instructions on how to use Endpoint Detection and Response solutions, Scripts, Splunk queries, YARA rules, network and Snort signatures to detect web shells.

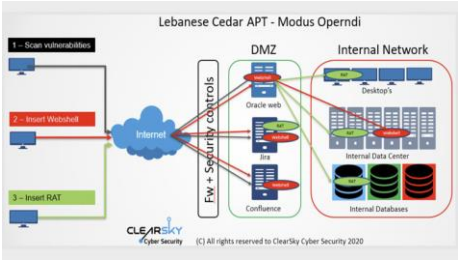
Web shells are scripts or tools that are deployed on hacked servers to gain and/or maintain access, to remotely execute arbitrary commands or code to deliver additional malicious payloads.

Malware Bytes

Volatile Cedar: The Emerging Threat

Source: https://www.hackread.com/

Israeli cybersecurity firm ClearSky has revealed that an APT group affiliated with Hezbollah Cyber Unit, called Volatile Cedar or Lebanese Cedar has been targeting companies around the world to extract valuable information. According to report, a new version of explosive malware RAT has been developed by the APT group and stealthily hacking businesses worldwide by stealing sensitive data like intelligence information, call records, etc. In case its target is a telecommunication firm, the group frequently performs espionage operations. Threat Actors gain initial foothold using three flaws (CVE-2019-3396, CVE-2019-11581 and CVE-2012-3152) in the unpatched Oracle and Atlassian web servers. The attackers then injected a web shell and a JSP file browser which were used to fetch additional malware and download the Explosive RAT, which comes with capabilities to capture screenshots, record keystrokes and execute arbitrary commands on victim's system.



Threat Actors gain initial foothold using three flaws (CVE-2019-3396, CVE-2019-11581 and CVE-2012-3152) in the unpatched Oracle and Atlassian web servers.

Malware uses Wi-Fi BSSID for Victim Identification

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

Security researchers have discovered a new malware strain that relies on grabbing infected users' Basic Service Set Identifier (BSSID). BSSID is MAC physical address of the wireless router or access point the user used to connect via Wi-Fi. Malware after collecting BSSID used to check geographical location of victim using free BSSID-to-geo database. This database is a collection of known BSSIDs and their geographical location. Checking BSSID against this database allow malware to effectively determine the physical geographical location of Wi-Fi access point. These

Malware after collecting BSSID used to check geographical location of victim using free BSSID-to-geo database.

collected data is used by state sponsored actors for their operations.

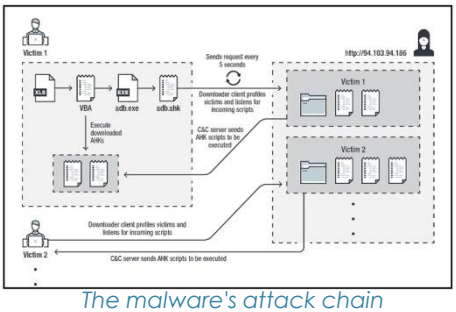
Image Source: thehackernews.com

This self-decoding technique acts as unpacker stub that is executed upon opening the document.

North Korea-linked APT37 targets South with RokRat Trojan

Source: https://securityaffairs.co/

Researchers from malware bytes found a campaign targeting South Korean government with revised version of RokRat RAT trojan. In past attacks, this trojan was attached to APT37. It uses a VBA self-decoding technique to decode itself directly into the memory of the victim's machine. This self-decoding technique acts as unpacker stub that is executed upon opening the document. It unpacks the macro and inject it into the memory of Microsoft office to avoid detection. The stub then embeds a variant of the RokRat into Notepad. The threat actor bypasses the VB object model by modifying its register value. The shellcode injected into Notepad.exe process downloads an encrypted payload. RokRAT is able to steal data from infected systems and send it to cloud based services.



The malware's attack chain

The info-stealer directly downloads and executes AHK scripts to execute different activities. By doing this, the attacker makes decision to upload a specific script to achieve customised tasks for each user or group of users.

New AutoHotkey-Based Malware Targets US, Canadian Banks

BFSI Sector, NCIIPC

In an ongoing attack campaign that started in early 2020, threat actors were found to be distributing this info stealer, focusing on customers of financial organisations located in the U.S. and Canada. The new malware is written in AutoHotkey or AHK, which is an open-source scripting programming language, used for software automation for Windows operating system. It provides easy keyboard shortcuts or hotkeys and fast micro-creation. The malware allows users to create a compiled .EXE with their codes inside.

Malware Capabilities: The malware infection consists of multiple stages that start with an email as a malicious excel file. The file contains a script compiler executable, which is a malicious script file. When file is opened and executed, it brings a hotkey downloader into the victim's devices. The downloader consists of multiple malware components designed to achieve persistence, profiling victims and downloading and executing additional scripts. In the next stage of the attack, the malware downloads the browser credential stealer, to take the encrypted credentials from various browsers. In the final stage of the attack, the malware decrypts the exfiltrate data and sends it to the command-and-control servers via a POST method. Uniqueness to this malware is reliance on AHK files to receive commands instead of a command-and-control server. The info-stealer directly downloads and executes AHK scripts to execute different activities. By doing

this, the attacker makes decision to upload a specific script to achieve customised tasks for each user or group of users. This prevents the main components being exposed in public, specifically to researchers or to sandboxes.

Recommendation: Scripting language allows attacker to hide their intention from sandboxes, making the attacks more sophisticated and deadly. Thus, cyber awareness and training about the risks and challenges associated with macro-laced email attachments to employees, use of trustworthy anti-malware software and stay away alerts while opening emails from unknown senders is recommended.

Scripting language allows attacker to hide their intention from sandboxes, making the attacks more sophisticated and deadly.

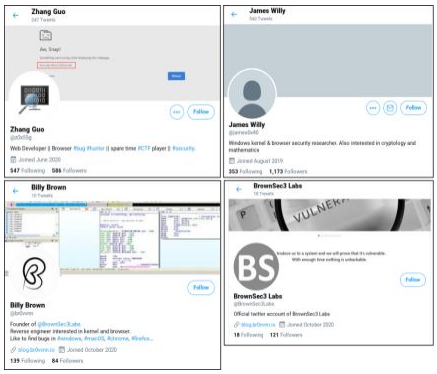
References:

[1] https://securityaffairs.co/wordpress/112895/malware/credential-stealer-banks.html

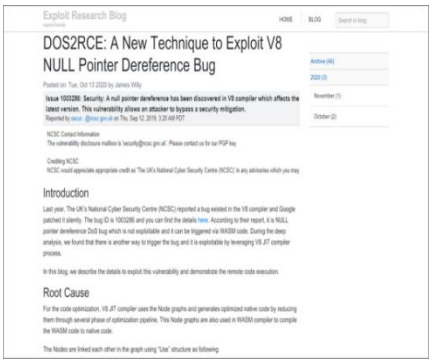
[2] https://www.bankinfosecurity.in/new-autohotkey-based-malware-targets-us-canadian-banks-a-15680/

Suspected North Korea linked group targets Security Researchers

Source: https://blog.google/



Suspected threat actor group linked to DPRK is targeting security researchers with an associate social-engineering campaign that sets up trustworthy relationships with them and then infects their organisation's systems with custom backdoor malware. To build credibility and connect with security researchers, they established a research blog and multiple Twitter profiles to interact with potential targets however, the attackers did not limit themselves to Twitter, their identities found out across Telegram, Keybase, LinkedIn, and Discord also, messaging established security researchers about potential collaborations. They also built a legitimate-looking blog, contains the different types of vulnerability analysis that find from a real firm. During their campaign, they claim that they found a flaw in Microsoft Window, or Chrome, depending on the expertise of their targets, and then needed help deciding if it had been exploitable. In addition to targeting users via social engineering, Google Threat Analysis Group (TAG) has also observed several cases where researchers have been compromised after visiting the threat actor's blog. The researchers have followed a link on Twitter, some malicious service was installed on the researcher's system to start beaconing to a threat actor-owned command and control server.



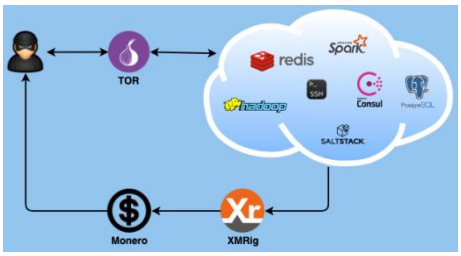


Figure-1: DreamBus botnet architecture

DreamBus: A New Threat to Linux Systems

Source: https://www.techradar.com/

DreamBus is a botnet capable of propagating itself both across the web and laterally through compromised internal networks employing a style of techniques. DreamBus targets enterprise-level apps that run on Linux systems. Targets consists a large collection of apps, like PostgreSQL, Redis, Hadoop YARN, Apache Spark, HashiCorp Consul, SaltStack, and also the SSH service. It is a variant of an older botnet named SystemdMiner but current DreamBus versions have received several improvements compared to initial SystemdMiner sightings. The cybercriminals deploying DreamBus do so with the aim of gaining an edge on Linux servers where they will download and install an open-source app used for mining the cryptocurrency Monero. Further each infected server then becomes a part of the botnet. A number of these apps are targeted with brute-force attacks against their default administrator usernames, others with malicious commands sent to exposed API endpoints, or via exploits for older vulnerabilities.

DreamBus targets enterprise-level apps that run on Linux systems. Targets consists a large collection of apps, like PostgreSQL, Redis, Hadoop YARN, Apache Spark, HashiCorp Consul, SaltStack, and also the SSH service.

Botnet architecture: DreamBus includes a modular design with regular deployment of latest modules and updates. Most command-and-control components are hosted through TOR or on an anonymous file-sharing service. Figure-1 shows a high-level diagram of the DreamBus botnet architecture and its various modules.

Key Points:

- DreamBus may be a modular Linux-based botnet with worm-like behavior that has been around a minimum of since early 2019.
- The malware can spread to systems that are not directly exposed to the internet by scanning private RFC 1918 subnet ranges for vulnerable systems.
- DreamBus uses a mix of implicit trust, application-specific exploits, and weak passwords to achieve access to systems like databases, cloud-based applications, and IT administration tools.
- The botnet is currently monetized through leveraging infected systems to mine Monero cryptocurrency using XMRig.
- The threat actor operating DreamBus appears to be located in Russia or Eastern Europe supported the time of deployment for new commands.

DreamBus uses a mix of implicit trust, application-specific exploits, and weak passwords to achieve access to systems like databases, cloud-based applications, and IT administration tools.

Networks Still Host Devices Infected with VPNFilter Malware

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

According to researchers at a cybersecurity firm VPNFilter malware is present in hundreds of networks. Malicious actor could take control of these infected devices. It targets a large number of

routers and Network Attached Storage (NAS) device from ASUS, D-Link, Huawei, Linksys, MicroTik, Netgear, QNAP, TP-Link etc. VPNFilter first attempts to obtain the address of its C&C server from various sources. This malware has extensive capabilities such as exfiltrate data, encrypt communications with command and control (C&C) server, map networks, exploit endpoints connected to infected devices, find additional victims and create a network of proxies for future use. These infected networks can be easily taken over by any threat actor with knowledge of how the VPNFilter works. The original actor can also take control of these devices at any point of time. This problem could be solved through firmware updates.

According to researchers at a cybersecurity firm VPNFilter malware is present in hundreds of networks. Malicious actor could take control of these infected devices.

Sunspot, Third Malware involved in SolarWinds Supply Chain Attack

Source: https:// https://securityaffairs.co/

According to Cybersecurity firm Crowdstrike, a third malware dubbed as SUNSPOT was found involved in SolarWinds supply chain attack. SUNSPOT monitors running processes involved in compilation of the Orion Product and replaces one of the source files to include backdoor code. The Sunspot malware was installed on SolarWinds build server. Sunspot used to watch the build server for build commands that assembled Orion. This malware replaces source code files inside the Orion app with files that loaded the Sunburst malware. SolarWinds hackers are tracked under different names such as UNC2452, DarkHalo and StellarParticle. Several safeguards were added to SUNSPOT to avoid the Orion builds from falling, potentially alerting developers to the adversary's presence.

The Sunspot malware was installed on SolarWinds build server. Sunspot used to watch the build server for build commands that assembled Orion.

Red Echo's Shadow Pad Malware

Source: https://www.oneindia.com/, https://www.news18.com/

Shadow Pad is one of the largest known supply-chain attacks that delivers backdoor Trojan hidden in modified versions of software. Once inside a system, the malware can upload files, create processes, and store information. Recently, alleged Chinese government-linked group of hackers called Red Echo targeted India's critical power grid system through this malware. The national power grid operator and its regional units have along with other critical sector organisations been alerted about the malware campaign along with suspected IPs & domains involved in the campaign. Flow of Malware was pieced together by Recorded Future, a US based company that studies state actor sponsored cyber-attack campaigns worldwide.

Shadow Pad is one of the largest known supply-chain attacks that deliver a backdoor Trojan hidden in modified versions of software. Once inside a system, the malware can upload files, create processes, and store information.

Learning

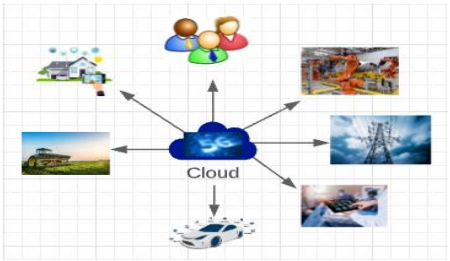
ENISA releases new Guidelines for Navigating Cyber Risk

Source: https://www.enisa.europa.eu/

The European Union Agency for Cybersecurity (ENISA) has released cybersecurity guidelines to help European port operators manage cyber risks amid digital transformation and increased regulations. The guidelines encourage port operators to develop a set of good practices to help them identify and evaluate cyber risks, and effectively identify suitable security measures. The practices include:

The guidelines encourage port operators to develop a set of good practices to help them identify and evaluate cyber risks, and effectively identify suitable security measures.

- Identify cyber-related assets and services in a systematic way, for example maintaining an asset inventory, identifying dependencies and deploying automation.
- Adopt a comprehensive approach to identify and evaluate cyber risks that includes risk indicators and business impact analysis, involves all relevant stakeholders and is integrated at an organisational level.
- Prioritise the implementation of security measures following a risk-based approach that considers security measure effectiveness and pertinence to the identified risks, and is founded in a security-by-design approach.
- Implement organisation-wide cybersecurity awareness and technical training programmes.
- Develop a comprehensive cybersecurity programme that involves a commitment by senior management.
- To identify priorities for improvement, and budget and resource allocation through cybersecurity maturity self-assessment.



Security issues in 5G-enabled IoT Network/Devices

VAPT Team, NCIIPC

IoT refers to a set of physical devices connected together with unique IP Addresses and are accessible through the internet. It provides an ease to access information remotely and efficiently in a cost-effective manner as well as helps to build/support an automated infrastructure. 5G Mobile communication system has elevated the demand for IoT products by overcoming significant challenges such as data transfer rate, latency, expansion of the network, support for heterogeneous services with massive multiple inputs multiple outputs (MIMO), and many more. It also facilitates uninterrupted and consistent connectivity for a range of

applications. It has enabled I-IoT to exploit its maximum potential which is a merger of AI and IoT. The low latency feature of 5G has opened the door for remote surgery with the help of different robotic components. Internet of Drones (IoD) needs an efficient network where handoffs are smooth and transmission of data at higher rates and consumes less power, 5G serves the purpose. Considering the trends and popularity It is expected that very soon IoT will be ubiquitous and hence security issues related to IoT become extremely critical. There are already existing security issues and possible attacks in 5G enabled IoT networks. Popular possible attacks and their intensity are listed in table-1. The heterogeneity and openness of IoT networks have created complex challenges for researchers to come up with security solutions against advanced state-of-the-art cyber-attacks. The attacks on the IoT net-works could be so disastrous that they can pose threat to lives. The efficiency of healthcare smart devices has improved and at the same time, these devices are prone to attacks. IoT devices are dependable, hence security must be ensured at the device level to maintain the functionality of the network. Security protocols have been incorporated in 5G to counter the cyber-attacks. Some existing protocols for security are tabulated in table-2. The existing protocols are not enough to provide robust security mechanisms to protect the IoT enabled network from a wide range of attacks. It opens a door for researchers to look beyond and come up with new solutions. The protocols must have less computational complexity considering that the network nodes have limited computational capability, storage, and endurance time.

Types	Description	Intensity/Threat
Eavesdropping	5G enabled IoT networks are prone to sniffing subject to advanced cyber-attacking tools and tuning to exact frequencies	• Privacy Invasion/ Data Breach • Unauthorized network monitoring • Further advanced attacks
Replay Attack	Interception of exchanged message incorporating delays or retransmission	• Unexpected latency and delays • Bandwidth loss • Service unavailability
Impersonation Attack	Determines the identity of communicating parties	• Identity disclosure smart IoT device • Targetted cyber-attack execution • Stepping stone to further attacks
Denial of Service Attack	Vengeful tasks are performed to stop the communication between genuine parties	• Resource unavailability • Bandwidth loss. • Malfunctioning of IoT device
Database Attack	Databases are prone to attacks such as SQL, XSS and CSRF which are still persistent	• Sensitive Information disclosure • Stealing of Database resources • Database modifications
MITM Attack	Interceptions of transmitted message and further modifications in the information	• Integrity violation • Privacy Invasion/Information leakage • Resource hijacking
Malware Attack	Malicious scripts can be embedded in existing network to perform desired cyber-attacks.	• Unauthorised access to the IoT devices • Control over resources • Malfunctioning of network/devices.

Table-1

Security Protocols	Description
Intrusion detection protocols	It facilitates verification of the ongoing traffic and act accordingly such as, blocking the malicious IP or send the information to the administrator.
User Authentication /Device Authentication	Mutual authentication of devices helps each other to keep track of identities to avoid any unauthorized access.
Access Control/User access control	The limitations over access to the network resource or network device is implemented with this protocol.
User domain security	It incorporates hardware security mechanisms to protect devices from any alterations.
Key management	The system takes care of generation, exchange, usage and revocation of keys.

Table-2

The existing protocols are not enough to provide robust security mechanisms to protect the IoT enabled network from a wide range of attacks.

References:

[1] Mohammad Wazid, Ashok Kumar Das, Sachin Shetty, Prosanta Gope, and Joel J.P.C. Rodrigues''Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap '' in IEEE Access, Volume 9, pp 4466-4489, Dec, 2020

[2] R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions recent advancements and future directions", IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 196-248, 1st Quart. 2020.

[3] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5G security challenges and solutions", IEEE Commun. Standards Mag., vol. 2, no. 1, pp. 36-43, Mar. 2018

[4] Pros & Cons of Internet of Things, Oct. 2018, [online] Available: https://www.redalkemi.com/blog/post/pros-cons-of-internet-of-things.

[5] Unlocking IoT Data With 5G and AI, Oct. 2019, [online] Available: https://innovate.ieee.org/innovation-spotlight/5g-iot-ai/

Cloud Security Issues and Guidelines

S&PE Sector, NCIIPC

Cloud security involves combination of different technologies, policies, controls, and services to protect the stored data, hosted applications, and the back-end infrastructure from cyberattacks. The need of adopting security controls for Cloud environment is exponentially increasing with the rapid growth of popular service-based models IAAS, PAAS, etc. Organisations have started using cloud platform in the following three major service models such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). There are 4 essential pillars of cloud security:

- Network protections.
- Visibility and compliance.
- Identity security.
- Compute-based security.

Organisations have started using cloud platform in the following three major service models such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

The identified challenges comprising the trends and obstacles regarding cybersecurity and data protection of cloud security are as follows:

Cloud security challenges

- Lack of trust of Cloud solutions
- Lack of security and technology expertise
- Cybersecurity investment is not a priority
- Proving regulatory compliance of the CSP
- Integration of Cloud with legacy systems difficulties

Data Protection challenges

- Privacy by design techniques
- Data governance
- Data deletion
- Encryption

Some of the cloud security threats and solutions are as follows:

Regular backups should be performed by organisations and every backup should be stored offline or on a separate network. It is better to recover data from backup rather giving ransom.

- Malware and Ransomware Attacks: One of the most common and rising cybersecurity threats in the past few years are ransomware attacks. Ransomware also accounted for malware attacks. Data can be exfiltrated from cloud services using malware which is spread from attackers. Regular backups should be performed by organisations and every backup should be stored offline or on a separate network. It is better to recover data from backup rather giving ransom.
- Data Theft and Breaches: Data breaches are increasing and has impact over individuals as well as organisations. Weak cloud security measures include storing unencrypted data or

there is no multi-factor authentication to gain access to the service. Encryption helps in mitigating data breaches. By encryption data is protected from attackers by making data unreadable by the attacker.

- End-user control: There is a risk of workers or employees using the cloud could share or expose the data. In return this might bring contract breaches with clients and/or business partners.
- Network reliability (latency, performance): Non reliable network impacts the kind of services delivered. Network reliability vastly revolves around design.
- Insecure APIs: Cloud services can be customised through API or Application Programming Interfaces. However, they can be threat to cloud security due to their very nature.

Encryption helps in mitigating data breaches. By encryption data is protected from attackers by making data unreadable by the attacker.

Besides these data privacy, lack of control since data is managed by someone else, use of shared servers, lack of backup services, usage of rogue devices and usage of insecure APIs and gateways are some of the reasons for mentioned cloud security threats. Following security & data protection measures can be implemented:

- Identify data protection & security requirements such as legislation, internal policies & legal requirements.
- Conduct risk assessment & data-protection impact assessment
- Ensure the business-continuity & disaster-recovery
- Ensure the organisation's data is either deleted if retention period has expired or removed upon termination of contract.
- Ensure that the incident response (IR) plan defines all the actions to be taken after a security incident.
- Identify the requirements for event logging & continuous monitoring.
- Identify and setup all the processes for vulnerability & patch management.
- Identify asset inventory & classify data stored in cloud environments should be monitored & recorded.
- Ensure data transfer is encrypted from-and-to the cloud service for all incoming & outgoing connections.
- Ensure all data is provided in industry-standard format from the Cloud service provider.
- Identify asset inventory all devices and endpoints and define a security baseline for hardening these asset inventory.
- Ensure that the access to cloud services is secured by strong authentication controls.

Ensure the organisation's data is either deleted if retention period has expired or removed upon termination of contract.

Ensure data transfer is encrypted from-and-to the cloud service for all incoming & outgoing connections.

- Establish a regular target group-oriented awareness and training program for all internal and external employees which deal with sensitive data such as electronic health records or medical diagnosis.
- Ensure traffic between untrusted and trusted connections of network environments and virtual instances is restricted and monitored.

Ensure traffic between untrusted and trusted connections of network environments and virtual instances is restricted and monitored.

References:

[1] https://www.tripwire.com/state-of-security/healthcare/enisa-releases-guidelines-cloud-security-healthcare-services/?web_view=true

[2] https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/

[3] https://solutionsreview.com/cloud-platforms/7-cloud-storage-security-risks-you-need-to-know-about/

[4] https://www.tripwire.com/state-of-security/featured/6-cloud-security-threats-healthcare-companies-face-solutions/

DDoS Attack: How DDoS Attacks are Evolving

Threat Assessment Team, NCIIPC

A distributed denial of service (DDoS) attack is an attack when an attacker tries to make it difficult for a service to be delivered which is achieved by blocking access to devices, servers, services, applications, networks, and even specific transactions within applications. In a DoS attack, one system sends the malicious data or requests while DDoS attack comes from multiple systems. As a result, the available ICT resources become inaccessible due to excessive utilization. Types of DDoS attacks:

- Volume-based attacks use massive amounts of spurious traffic, measured in bits per second (bps), to overwhelm any critical resource such as a website or server using ICMP, UDP and spoofed packet flood attacks.
- Application-layer attacks are conducted by flooding applications with maliciously crafted requests measured in requests per second (RPS).
- Protocol or network-layer DDoS attacks send large numbers of packets measured in packets per second (PPS) to targeted network infrastructures and infrastructure management tools using protocol attacks like Smurf DDoS and SYN floods.

Application-layer attacks are conducted by flooding applications with maliciously crafted requests measured in requests per second (RPS).

DDoS attack symptoms and tools: DDoS attacks may appear as

non-malicious activity which will cause availability issues –like a downed server or system, too many legitimate requests from legitimate users, or even a cut cable. DDoS attackers typically depend on centrally controlled botnets which are harvested by identifying vulnerable systems that they can infect through malvertising attacks, phishing attacks and other mass infection techniques.

How DDoS attacks evolve: It's becoming more common for DDoS attacks to be conducted by rented botnets. Another trend observed is that the use of multiple attack vectors within an attack, also referred to as Advanced Persistent Denial-of-Service APDoS. For example, an APDoS attack include attacks against applications and databases as well as directly on the server. DDoS attackers not only directly target their victims but also the organisations on which they depend like cloud providers and ISPs.

Another trend observed is that the use of multiple attack vectors within an attack, also referred to as Advanced Persistent Denial-of-Service APDoS.

The addition of new IoT devices, rise of machine learning and AI will all play a key role in changing these DDoS attacks. Attackers will eventually integrate these newer technologies into attacks making it harder for defenders to capture DDoS attacks, specifically those attacks that cannot be ceased by simple ACLs or signatures. DDoS defence technology will have to evolve in that direction to mitigate DDoS attacks.

Attackers will eventually integrate these newer technologies into attacks making it harder for defenders to capture DDoS attacks, specifically those attacks that cannot be ceased by simple ACLs or signatures.

References:

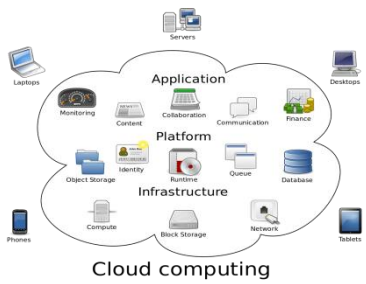
[1] https://www.csoonline.com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving.html#:~:text=A%20distributed%20denial%20of%20service,a%20service%20to%20be%20delivered.&text=In%20a%20DoS%20attack%2C%20it's,attack%20comes%20from%20multiple%20systems.

[2] https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/

[3] https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained

Cloud Computing: Possible Threats and their Mitigation

Government Sector, NCIIPC



Cloud computing is the on-demand availability of computing system resources, mainly computing power and data storage etc. It provides a flexible model for IT management with features like remote working, mobility, need based elasticity and cost effectiveness. There are several potential threats on Cloud security like data breaches, malicious insiders, account hijacking, and

DDoS attacks. Cloud computing may experience the following vulnerabilities:

Insecure Application user interfaces (APIs) can open lines of communications for attackers to exploit cloud resources.

- Insecure Application User Interfaces can open lines of communications for attackers to exploit cloud resources.
- Threats associated with data deletion exists because the consumers have reduced visibility into where their data is physically stored in the cloud.
- Organisations migrating to the cloud often perform insufficient due diligence. The users are moving data to the cloud without perception of the full scope of doing so, the security measures used by the CSP, and their own responsibility to provide security measures.
- There is a rich source of stolen data for cybercriminals in cloud storage. The prominent types of cloud misconfiguration that enterprises encounter are as follows:
    - Any misconfiguration in the cloud security groups may allow an attacker to access your cloud-based servers and exfiltrate data and credentials.
    - Insecure cloud storage buckets can result in attackers gaining access to data stored in the cloud and downloading confidential data, which can have devastating consequences for organisation.

Insecure cloud storage buckets can result in attackers gaining access to data stored in the cloud and downloading confidential data, which can have devastating consequences for organisation.

- Intellectual property and data in a cloud environment is vulnerable to security threats, especially if the data is stored online.
- Enterprises must have steadfast rules for Compliance Violations and Regulatory Actions.
- Unawareness among employees to use cloud computing services may leads loss of control over their data assets and eventually become vulnerable to breaches and insider security threats.

Preventive Measures and Mitigation strategies:

APIs must be secured with strong authentication, encryption, activity monitoring, and access control. It is recommended to use SSL/TLS encryption for data-in-transit.

- Double-check cloud storage security configurations upon setting up a cloud server.
- APIs must be secured with strong authentication, encryption, activity monitoring, and access control. It is recommended to use SSL/TLS encryption for data-in-transit. Implement Captcha, multi-factor authentication with schemas such as one-time passwords and limit the login times, digital identities to ensure strong authentication controls.
- Encrypt the data, back up in offline regularly and geo-diversify vital data. Use Data Loss Prevention (DLP) software to detect and prevent unauthorized movement of sensitive data.

- Know all of your users, roles, and access permissions, have a clear identity, be able to track all assets across all geographic locations. There is a need of maintaining strong configuration management and implement an incident response plan for violations related to cloud computing.
- Conduct regular audit of servers, scan routinely for security risks and vulnerabilities, limit the access to security system and privileged central servers and provide adequate training on various security aspects to protect confidential information.

It is recommended to conduct regular audit of servers, scan routinely for security risks and vulnerabilities, limit the access to security system and privileged central servers and provide adequate training on various security aspects to protect confidential information.

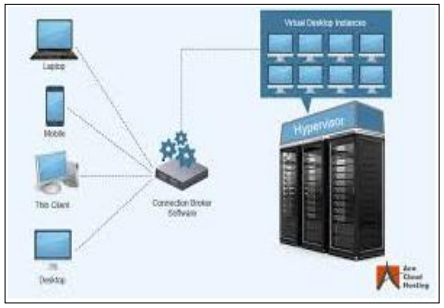
References:

[1] https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html

[2] https://www.infoq.com/articles/ieee-cloud-computing-vulnerabilities

Virtual Desktop Cyber Security

Transport Sector, NCIIPC



In Virtual Desktop Infrastructure, user's desktop environment (the icons, wallpaper, windows, folders, toolbars, widgets, etc.) is stored remotely on a server, rather than on a neighbourhood PC or other client device. Desktop virtualization software isolates the desktop operating systems, applications and data from the hardware client, storing the "virtual desktop" on an out of doors server. Cybersecurity is one altogether IT's top priorities. Security severance is devastating to an enterprise. While no system is guaranteed 100% secure, IT sector has endless challenged with ensuring maximum security. Cyber attackers are perpetually looked for infrastructure penetration. Locking down the virtual desktop and accelerating system security is top of mind of IT but ignoring the user facet of security is harmful. It is vital to educate users about phishing emails, fraudulent phone calls requesting passwords, screen visibility security and similar tactics because these represent the foremost vulnerable aspects of any desktop security and virtual desktops don't seem to be any different. Virtual desktops can easily expose a corporation to the next security threats:

Desktop virtualization software isolates the desktop operating systems, applications and data from the hardware client, storing the "virtual desktop" on an out of doors server.

- Ransomware
- Malware
- Insider threats
- Network sniffing

Virtual Desktop security risks: Virtual desktops can present unique security risks which are key points of vulnerability:

- The hypervisor
- The network

- The end users
- Unpatched VMs

Few ways to boost virtual desktop Cyber Security and ensure business continuity:

- Recognizing threats ranging from firewall attacks to phishing emails to system infiltrations, utilised by cyber attackers, is that the initiative in preventing them.
- To forestall the user device from serving as a conduit, when features like USB devices and device ports are enabled, system lockdown policies should be enabled to eliminate unneeded peripherals from being mapped.
- Strict password policies, timeouts, and capabilities like copy/paste is additionally controlled by configuring Group Policy Objects (GPOs) within Active Directory.

VDI security best practices: Securing a virtualized environment requires quite cutting-edge tools. Best practices can go a protracted way toward safeguarding mission-critical systems and confidential data. These include:

Securing a virtualized environment requires quite cutting-edge tools. Best practices can go a protracted way toward safeguarding mission-critical systems and confidential data.

- Setting controls to disable a tool in local mode if it is not synchronized within a predetermined interval. This allows companies to stay before hackers on the lookout for innovative ways to outsmart security protocols.
- Quarantining intrusions with micro-segmentation in order that they don't spread across the network.
- Investing in employee training to attenuate data leakage from lost or stolen devices.
- Ensuring endpoint protection by applying the latest security patches to operating systems, constantly updating antimalware software, and taking advantage of an endpoint device's built-in, hardware security capabilities.

Major security benefits of virtual desktop infrastructures are as under:

Virtual desktops help lower the costs of disaster recovery and business continuity processes.

- Virtual desktops and virtual workspaces are dynamically created from compliant copies of operating systems, applications and user profiles.
- Disaster recovery: Virtual desktops help lower the costs of disaster recovery and business continuity processes. it's visiting be hosted in any corporate data centre; IT teams can quickly move a virtual machine to a healthy host if the one it currently resides on experiences a hardware failure.
- Data security: Employees are less likely to fall victim to data theft whereas, sensitive data remains within the info centre where security can protect against leaks on endpoint devices.

- IT control: USB access, print capabilities and cut-and-paste including IP address, for consistent policy-based access control could be enable or disable automatically.

References:

[1] https://cio.economictimes.indiatimes.com/news/digital-security/tips-for-better-virtual-desktop-security/80164307

[2] https://searchsecurity.techtarget.com/tip/Security-benefits-of-vertual-desktop-infrastructures

[3] https://www.vmware.com/topics/glossary/content/virtual-desktop-infrastructure-security

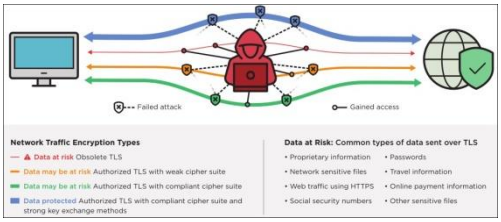
[4] https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide

Employees are less likely to fall victim to data theft whereas, sensitive data remains within the info centre where security can protect against leaks on endpoint devices.

NSA Shares Guidance to Mitigate Weak Encryption Protocols

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

The National Security Agency (NSA) has shared guidance to detect and replace obsolete Transport Layer Security (TLS) protocol versions with up-to-date and secure variants. NSA's guidance is targeted at Department of Defense (DoD), National Security System (NSS), and Defence Industrial Base (DIB) cybersecurity leaders, as well as network security analysts and system administrators. Implementing the measures in NSA's guidance eliminates the false sense of security provided by obsolete encryption protocols by blocking insecure cipher suites, TLS versions, and key exchange methods to encrypt network traffic properly. NSA recommends to use only TLS 1.2 or TLS 1.3 and not to use SSL 2.0, SSL 3.0, TLS 1.0, and TLS1.1. By using NSA's guidance, government network owners can make informed decisions to enhance their cybersecurity posture by allowing only authorised and strong encryption protocol configurations in their organisation's environments. Since these risks impact all networks, all network owners and operators should consider taking these actions to reduce their risk exposure and make their systems tough targets for malicious actors. Updating TLS configurations will provide government and enterprise organisations with stronger authentication and encryption to help them build a better defence against malicious attacks and protect crucial information.



By using NSA's guidance, government network owners can make informed decisions to enhance their cybersecurity posture by allowing only authorised and strong encryption protocol configurations in their organisation's environments.

Vulnerability Watch

Image Source: https://ps.w.org/

The privilege-escalation flaw exists in the Orbit Fox registration widget.

Critical WordPress-Plugin Flaw Found in 'Orbit Fox'

Source: https://threatpost.com/orbit-fox-wordpress-plugin-bugs/163020/

The researchers of Wordfence have discovered an authenticated privilege-escalation vulnerability that carries a CVSSv3 score of 9.9. The privilege-escalation flaw exists in the Orbit Fox registration widget. There is a lack of server-side validation in Orbit Fox, meaning lower-level contributors, authors and editors for the site could set the user role to that of an administrator upon successful registration. To exploit this vulnerability authenticated attackers with contributor level access or above can elevate themselves to administrator status and potentially take over a WordPress site.

This vulnerability is considered critical as it can be leveraged to completely compromise the vulnerable application as well as the underlying operating system.

Critical Vulnerability in DELL EMC Avamar Server

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-29495

DELL EMC Avamar Server contains an OS Command Injection vulnerability, CVE-2020-29495, in Fitness Analyzer. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS with high privileges. This vulnerability is considered critical as it can be leveraged to completely compromise the vulnerable application as well as underlying operating system. It has a CVSSv3 Score of 10.0.

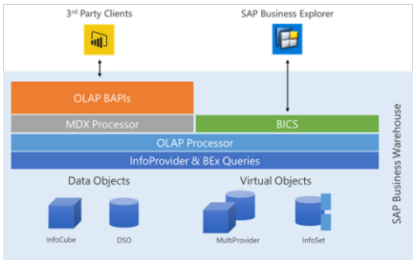


Image Source: https://docs.microsoft.com/

Vulnerability in SAP Business Warehouse

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-21465

The SAP Business Warehouse Database Interface allows an attacker with low privilege to execute any crafted database queries thereby exposing the backend database. An attacker can also include their own SQL commands which the database will execute without properly sanitizing the untrusted data leading to SQL injection vulnerability, CVE-2021-21465 with CVSSv3 9.9, can fully compromise the affected SAP system.

Event Viewer log showing NTFS corruption from command

"Critically Underestimated" NTFS Vulnerability

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

An unpatched zero-day in Microsoft Windows 10 allow attackers to corrupt an NTFS-formatted hard drive with a one-line command, with Windows prompting the user to restart computer to repair the corrupted disk records. This flaw became exploitable starting around Windows 10 build 1803, the Windows 10 April 2018 Update, and continues to work in the latest version. This vulnerability can be triggered by standard and low privileged user accounts on

Windows 10 systems. A drive can become corrupted by merely trying to access the $i30 NTFS attribute on a folder in a certain way. An example command that corrupts a drive- cd c:\$i30:$bitmap. The '$i30' string, is an NTFS attribute associated with directories that contains a list of a directory's files and subfolders. It is unclear why accessing this attribute corrupts the drive.

Microsoft Implements Zerologon Flaw 'Enforcement Mode'

Source: https://threatpost.com/

Microsoft has announced it will enable domain controller "enforcement mode" by default, a measure that would help mitigate the critical Zerologon flaw, CVE-2020-1472 having CVSSv3 10.0. The Domain Controller enforcement mode "will block vulnerable connections from non-compliant devices. This new implementation is an attempt to block cybercriminals from gaining network access to domain controllers, which they can utilise to exploit the Zerologon privilege-escalation vulnerability. It is advised that all Domain Controllers be updated with the latest security patch.

The Domain Controller enforcement mode "will block vulnerable connections from non-compliant devices.

Multiple Critical Vulnerabilities Discovered in Cisco Jabber

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

Multiple vulnerabilities have been discovered in Cisco Jabber for Windows, MacOS, and mobile platforms that could allow an attacker to execute arbitrary programs on the underlying operating system with elevated privileges or gain access to sensitive information. The vulnerabilities CVE-2020-27134, CVE-2020-27133, CVE-2020-27132, CVE-2020-27127 (all CVEs have CVSSv3 9.9) are independent on one another which indicates exploitation of one of the vulnerabilities is not required to exploit another vulnerability. These vulnerabilities are due to improper validation of message contents, improper handling of input to the application protocol handlers, improper validation of message contents, and improper handling of input to the application protocol handlers respectively.

Image Source: https://i.ytimg.com/

Critical Vulnerability in SAP NetWeaver AS JAVA

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-26829

The vulnerability CVE-2020-26829 allows a remote attacker to bypass authentication process in SAP NetWeaver AS JAVA. It exists due to an error when processing authentication requests within the P2P Cluster Communication component. A remote attacker can gain unauthorised access to the application and may compromise the server. It has CVSSv3 score of 10.0.

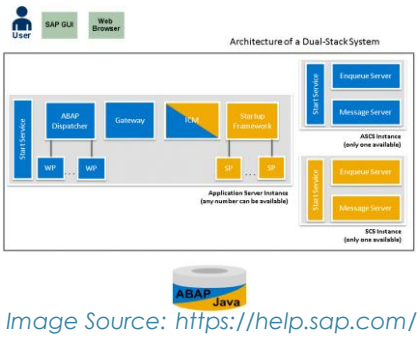


Image Source: https://help.sap.com/

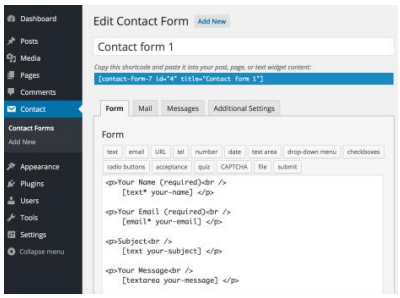


Image Source: https://ps.w.org/

Critical Vulnerability in Contact Form

Source: https://contactform7.com/

The CVE-2020-35489 vulnerability with CVSSv3 10.0 has been found in the WordPress plugin Contact Form 7 5.3.1 and older versions. This is an unrestricted file upload vulnerability that helps attackers to upload files of any type, bypassing all restrictions placed regarding the allowed upload-able file types on a website.

Image Source: https://dt-cdn.net/

Critical Vulnerability in SAP Commerce Cloud

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-21477

A Remote Code Execution vulnerability, CVE-2021-21477 has been discovered in SAP Commerce Cloud versions - 1808, 1811, 1905, 2005 and 2011. CVE-2021-21477 has CVSSv3 score of 9.9. Successful exploitation of this flaw could allow an attacker for remote code execution (RCE) that ultimately could compromise or disrupt the application. This vulnerability enables users with certain required privileges to edit drools rules. Using this privilege an authenticated attacker will be able to inject malicious code in the drools rules. Execution of this malicious code leads to Remote Code Execution vulnerability enabling the attacker to compromise the underlying host impairing confidentiality, integrity and availability of the application.

CVE ID	CVSSv3 Score	TCP/IP Stack analyzed	Description
CVE-2020-27213	7.5	Nut/Net 5.1	ISN generator relies on a highly predictable source (system timer) and has constant increments.
CVE-2020-27630	7.5	uC/TCP-IP 3.6.0	ISN generator relies on LCG, which is reversible from observed output streams. The algorithm is seeded with publicly recoverable information (i.e., system timer count).
CVE-2020-27631	7.5	CycloneTCP 1.9.6	ISN generator relies on LCG, which is reversible from observed output streams. The algorithm is initially seeded with a publicly observable CRC value.
CVE-2020-27632	7.5	NDKTCPIP 2.25	ISN generator is initialized with a constant value and has constant increments.
CVE-2020-27633	7.5	FNET 4.6.3	ISN generator is initialized with a constant value and has constant increments.
CVE-2020-27634	7.5	uIP 1.0 Contiki-OS 3.0 Contiki-NG 4.5	ISN generator is initialized with a constant value and has constant increments.
CVE-2020-27635	7.5	PicoTCP 1.7.0 PicoTCP-NG	ISN generator relies on LCG, which is reversible from observed output streams. The algorithm is seeded with publicly recoverable information (i.e., system timer count).
CVE-2020-27636	7.5	MPLAB Net 3.6.1	ISN generator relies on LCG, which is reversible from observed output streams. The algorithm is seeded with a static value.
CVE-2020-28388	6.5	Nucleus NET 4.3	ISN generator relies on a combination of values that can be inferred from a network capture (MAC address of an endpoint and a value derived from the system clock).

New vulnerabilities affecting TCP/IP stacks

Vulnerabilities in TCP/IP Stacks Open IoT, OT Devices to Attack

Telecom Sector, NCIIPC

TCP is a connection-oriented networking protocol to exchange data with two endpoints. It is used for error-free delivery of data at TCP/IP Transport Layer. Initial Sequence Number (ISNs) ensure that every TCP connection between two devices is unique and no collisions occurs between them. Additionally, it prevents third parties from interfering with an ongoing connection. To ensure these properties, ISNs must be randomly generated so that an attacker cannot guess an ISN and hijack an ongoing connection. Researchers have reported nine vulnerabilities affecting different TCP/IP stacks widely used in IoT and OT devices. These vulnerabilities are due to weak ISN generation and may be exploited for Denial of Service (DoS) attacks against the vulnerable devices or to inject malicious data on a device or even to bypass authentication. ElevenTCP/IP stacks, 7 of which are open-source (uIP, FNET, picoTCP, Nut/Net, lwIP, cycloneTCP, uC/TCP-IP) and the rest Microchip's MPLAB Net, Texas Instruments' NDKTCPIP, ARM's Nanostack and Siemens' Nucleus NET have been examined by researchers, who have concluded that lwIP and Nanostack are not vulnerable, however, the remaining are vulnerable due to non-implementation of Pseudo Random Number Generator

(PRNG) for ISN generation. These vulnerabilities allow attackers to predict the ISN of existing TCP connections or new ones.

Impact:

- By predicting the ISN of an existing TCP connection, attackers can close the session and execute a Denial-of-Service attack or attackers might hijack a session and inject malicious data. Data can be injected on sensitive unencrypted traffic like Telnet sessions (to inject commands), FTP file downloads (to serve malware) or HTTP responses (to direct the victim to a malicious page) etc.
- By targeting new TCP connections, an attacker may successfully complete a three-way handshake and spoof network packets intended for the victim endpoint or bypass address-based authentication and access control.

By predicting the ISN of an existing TCP connection, attackers can close the session and execute a Denial-of-Service attack or attackers might hijack a session and inject malicious data.

Recommendations for Network operators:

- Discover inventory devices, which runs on a vulnerable TCP/IP stack.
- Patch if possible: Monitor progressive patches released by affected device vendors and remedial plan for your vulnerable asset inventory balancing business risk and business continuity requirements.
- Segment to mitigate the risk: For vulnerable IoT and OT devices, use segmentation or separation to minimise their network exposure and the likelihood of compromise without impacting critical functions or business operations. It is also limiting the blast radius and business impact if a vulnerable device is compromised.
- Deploy IPsec: End-to-End cryptographic solutions built on top of the Network layer (IPsec) do not require any modifications to a TCP/IP stack in use while defending against TCP spoofing and connection reset attacks.

For vulnerable IoT and OT devices, use segmentation or separation to minimise their network exposure and the likelihood of compromise without impacting critical functions or business operations.

References:

[1] https://www.helpnetsecurity.com/2021/02/11/vulnerabilities-tcp-ip-iot/

[2] https://www.forescout.com/company/resources/numberjack-weak-isn-generation-in-embedded-tcpip-stacks/

OpenSSL 1.1.1k Patches Two High-Severity Vulnerabilities

Source: https://arstechnica.com/

OpenSSL Project has released its new version 1.1.1k, which patches two high-severity vulnerabilities. CVE-2021-3450, a vulnerability associated with verifying a certificate chain when using the X509_V_FLAG_X509_STRICT flag. In order to be affected, an application must explicitly set the X509_V_FLAG_X509_STRICT verification flag and either not set a purpose for the certificate verification or, override the default purpose, in the case of TLS

An OpenSSL TLS server could crash if sent a maliciously crafted renegotiation ClientHello message from a client.

client or server applications. CVE-2021-3449, a denial-of-server vulnerability is the result of a null pointer dereference bug. An OpenSSL TLS server could crash if sent a maliciously crafted renegotiation ClientHello message from a client. Servers running OpenSSL 1.1.1 are affected by CVE-2021-3449 if they have TLS 1.2 and renegotiation enabled, this is the default configuration. These two vulnerabilities have been rated as high severity.

Microsoft Exchange Server Vulnerabilities Patched

Source: https://msrc-blog.microsoft.com/

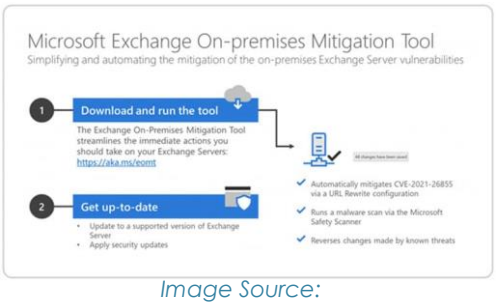


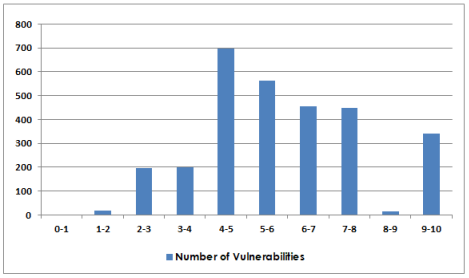
Image Source: https://3.bp.blogspot.com/

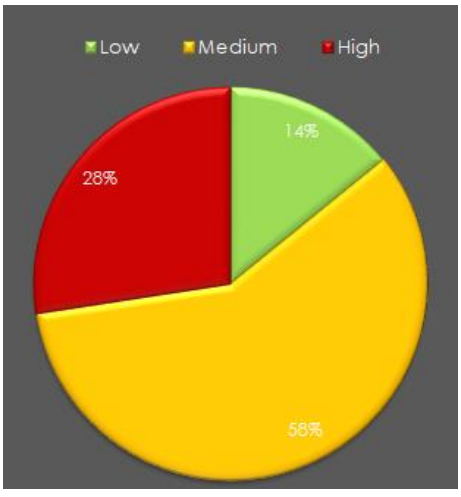
Microsoft addressed and patched vulnerabilities that were being exploited to attack on-premises versions of Microsoft Exchange Server. The recently exploited vulnerabilities are CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. These vulnerabilities are being exploited as part of an attack chain. The initial attack requires the ability to make an untrusted connection to the Exchange server, but other portions of the attack can be triggered if the attacker already has access or gets access through other means. These vulnerabilities affect Exchange Server versions 2013, 2016, and 2019, while Exchange Server 2010 is being updated for defence-in-depth purposes. These vulnerabilities can be mitigated using Exchange On-premises Mitigation Tool (EOMT). The Exchange On-premises Mitigation Tool automatically downloads any dependencies and runs the Microsoft Safety Scanner.

Quarterly Vulnerability Analysis Report

KMS Team, NCIIPC

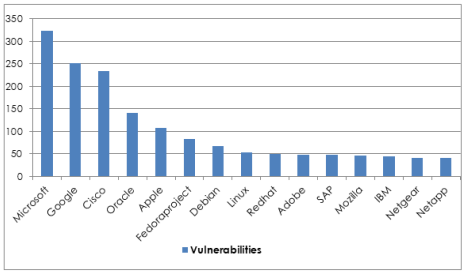
A total of 2936 vulnerabilities have been observed, out of which majority of vulnerabilities have score ranging from 4-7. 28 percent of total vulnerabilities reported were of high severity. Microsoft, Google, Cisco, Oracle and Apple were the top five vendors.





Severity	CVSS Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Dec'20	Jan'21	Feb'21		
Low	0-1	0	0	0	0	416
	1-2	4	5	10	19	
	2-3	111	45	40	196	
	3-4	88	58	55	201	
Medium	4-5	343	158	195	696	1715
	5-6	255	116	192	563	
	6-7	162	144	150	456	
High	7-8	188	114	147	449	805
	8-9	7	4	3	14	
	9-10	136	96	110	342	
Total		1294	740	902		2936

S. No.	Vendor	No. of Vulnerabilities			Total
		Dec'20	Jan'21	Feb'21	
1.	Microsoft	81	100	143	324
2.	Google	115	40	97	252
3.	Cisco	4	154	75	233
4.	Oracle	4	135	1	140
5.	Apple	69	2	36	107
6.	Fedoraproject	9	37	37	83
7.	Debian	26	18	23	67
8.	Linux	19	9	25	53
9.	Redhat	31	10	9	50
10.	Adobe	4	8	35	47
11.	SAP	12	27	8	47
12.	Mozilla	21	0	25	46
13.	IBM	24	1	19	44
14.	Netgear	41	0	0	41
15.	Netapp	0	40	1	41



Security App

Free Azure, Microsoft 365 Malicious Activity Detection Tool

Source: https://github.com/cisagov/Sparrow

The Cybersecurity and Infrastructure Security Agency's (CISA) Cloud Forensics team has created a free tool to help detect possible compromised accounts and applications in the Azure/m365 environment. The tool, Sparrow.ps1 has been developed with intention for use by incident responders, and focuses on narrow scope of user and application activity endemic to identity and authentication-based attacks seen recently in multiple sectors. This tool is neither exhaustive nor comprehensive of available data, and is used to narrow a larger set of available investigation modules and telemetry to those specific to recent attacks on federated identity sources and applications. Sparrow.ps1 checks and installs the required PowerShell modules on analysis machine, checks the unified audit log in Azure/M365 for certain Indicators of Compromise (IoC's), list Azure AD domains, and checks Azure service principals and their Microsoft Graph API permissions to identify any potential malicious activity. The tool then outputs the data into multiple CSV files that are located in user's default home directory in a folder called 'ExportDir'.

Image Source: 1.bp.blogspot.com

The tool, Sparrow.ps1 has been developed with intention for use by incident responders, and focuses on narrow scope of user and application activity endemic to identity and authentication-based attacks seen recently in multiple sectors.

Microsoft Sysmon Detects Malware Process Tampering Attempts

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

Sysmon 13 has been released by Microsoft with a new security feature that enables it to detect if a process has been tampered

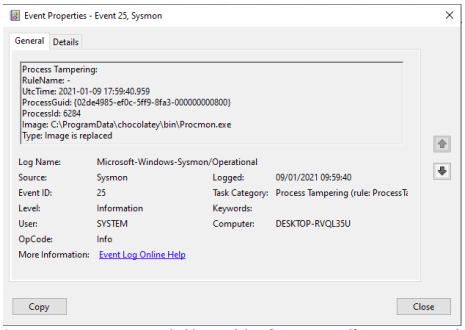


Image source: https://miro.medium.com/

using process herpaderping or process hollowing techniques. Sysmon also known as System Monitor is a Sysinternals tool designed to monitor systems for malicious activity and log those events to the Windows event log. In order to enable the process tampering detection feature, administrators need to add the 'ProcessTampering' configuration option to a configuration file. Once started, Sysmon will install its driver and begin collecting data quietly in the background. Sysmon will only monitor the basic events such as process creation and file time changes without a configuration file. All Sysmon events are logged to 'Applications and Services Logs/Microsoft/Windows/Sysmon/Operational' in the Event Viewer. With the ProcessTampering feature enabled, when process hollowing or process herpaderping is detected, Sysmon generates an 'Event 25 - Process Tampering' entry in Event Viewer.

FireEye releases New Tool in Response to SolarWinds Hack

Source: www.securityweek.com/, www.bankinfosecurity.asia/

FireEye researchers have released a free tool designed to check Microsoft 365 tenants for the use of techniques associated with UNC2452 (SolarWinds hacker group). This new tool is named Azure AD Investigator. It allows organisations to check their Microsoft cloud environments for evidence of an attack by SolarWinds hackers, and alerts security teams if it identifies artifacts that may require further review to determine their legitimacy. Azure AD Investigator is available on GitHub. This auditing tool can spot four attack tactics used by SolarWinds hackers to move laterally within the Office 365 cloud environment:

It allows organisations to check their Microsoft cloud environments for evidence of an attack by SolarWinds hackers, and alerts security teams if it identifies artifacts that may require further review to determine their legitimacy.

- Stealing Office 365 Active Directory Federation Services token-signing certificates to forge tokens used for authentication.
- Targeting Microsoft Office 365 with higher access privileges.
- Adding or modifying trusted domains in Azure Active Directory to add a new identity that the attacker controls.
- Creating a backdoor on Microsoft Office 365 applications to read email, send email as an arbitrary user and access user calendars.

Snort 3 becomes Available

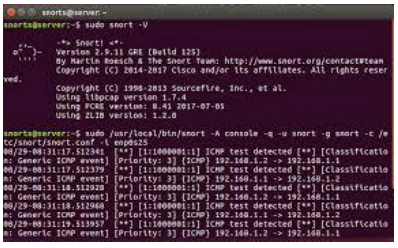


Image source: encrypted-tbn0.gstatic.com

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

Snort, developed by Cisco, provides real-time traffic analysis and packet logging capabilities. Snort 3 has now finally become generally available. The latest version of Snort provides faster and more efficient rules, it runs on multiple operating systems and environments, and it gives users more control. This version also provides support for multi-packet processing threads, autodetecting services for portless configuration, better cross-platform support, a shared configuration and attribute table,

scriptable configuration, pluggable key components, autogenerating reference documentation, and support for sticky buffers in rules.

Apple New Proxy Feature to Prevent Leaking IP Addresses

Source: https://gbhackers.com/apple-new-proxy-feature/

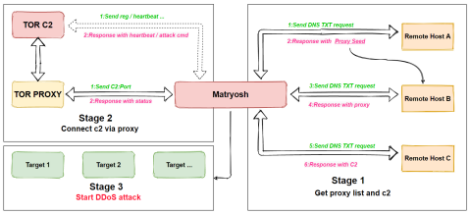
Image source: pbs.twimg.com/

Apple will soon roll out a feature in its upcoming iOS 14.5 update, which will ensure that it is unable to obtain the IP addresses of iOS users. All of Safari's Safe Browsing traffic will be re-routed through Apple-controlled proxy servers. This feature can be activated by activating the "Fraudulent Website Warning" option on Apple's iOS Safari settings on the iPhone and iPad. This feature will enhance and improve users' privacy while browsing using Apple's Safari.

Mobile Security

Matryosh Botnet

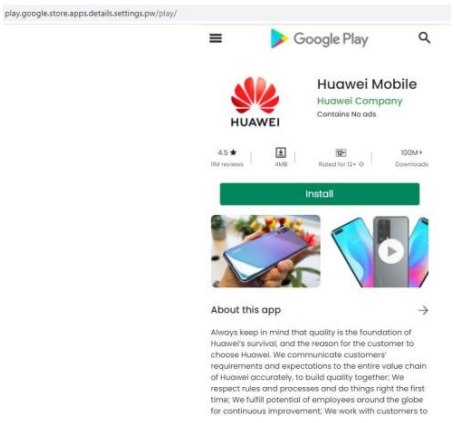
Source: https://blog.netlab.360.com/



Qihoo 360's Netlab researchers have discovered a new android botnet based on Mirai Framework, which propagates through Android Debug Bridge (ADB) interfaces. Dubbed as Matryosh, its main function is to facilitate DDoS attacks and it supports tcpraw, icmpecho, udpplain attacks. The botnet itself doesn't contain any exploitation module. It propagates via ADB and executes scripts downloaded from the remote host 199.19.226.25. The script consists of Matryosh samples of multiCPU architectures like x86, arm, mips etc. It uses TOR proxy to communicate with C2 and stores sensitive information in encrypted format. It is being speculated that it is the work of Moobot group.

Worm in WhatsApp

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



Researchers at ESET have discovered a new wormable malware spreading via WhatsApp in Android devices. Upon installation, it requests for notification access. It abuses WhatsApp's quick reply feature by automatically replying to any received WhatsApp messages and thus spreads to other contacts. To avoid suspicion, it maintains an hour gap before sending out messages of spreading itself. It sends a fake link of Huawei Mobile app which is hosted in a Google Playstore website lookalike. The app also requests permission for running in background and can spread overlays on other applications to steal credentials and sensitive information. It is currently believed to be an adware campaign.

Malware in Google PlayStore

Source: https://thehackernews.com/

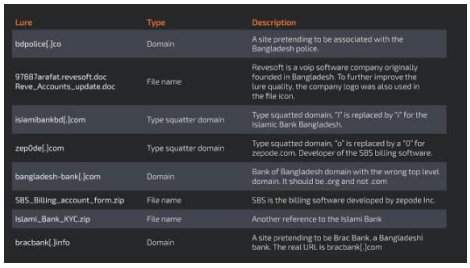
Cake VPN	com.lazycoder.cakevpns
Pacific VPN	com.protectvpn.freeapp
eVPN	com.abcd.evpnfree
BeatPlayer	com.crrl.beatplayers
QR/Barcode Scanner MAX	com.bezrukd.qrcodebarcode
eVPN	com.abcd.evpnfree
Music Player	com.revosleap.samplemusicplayers
tooltipnatorlibrary	com.mistergrizzlys.docscanpro
QRecorder	com.record.callvoicerecorder

It uses Firebase for C2 communication and downloads malicious payloads from GitHub.

Researchers at Check Point have recently discovered a new malware dropper dubbed as Clast82, targeting financial apps. Nine apps in Google PlayStore were found to be loaded with this malware. After escaping detection by Google Play Protect, it urges the victim to grant fake "Google Play Services" permission every five seconds, so that it can install AlientBot Banker and MRAT which steals credentials and 2FA codes from financial apps. When the app is posted for the first time in Google PlayStore, it doesn't contain any malware which in trust is used to gain popularity and trust. The unwanted code is added via app updates. It uses Firebase for C2 communication and downloads malicious payloads from GitHub.

LodaRAT for Android

Source: https://blog.talosintelligence.com/



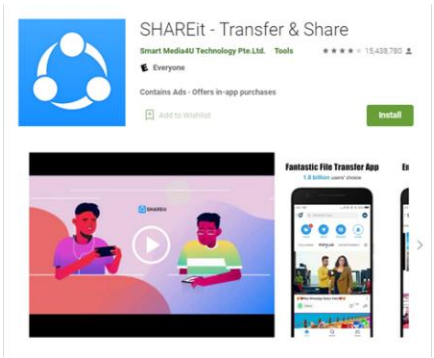
Lure	Type	Description
bdpolice[.]co	Domain	A site pretending to be associated with the Bangladesh police.
97887arafat.revesoft.doc Reve_Accounts_update.doc	File name	Revesoft is a voip software company originally founded in Bangladesh. To further improve the lure quality, the company logo was also used in the file icon.
isiamibankbd[.]com	Type squatter domain	Type squatted domain, "I" is replaced by "i" for Islamic Bank Bangladesh.
zep0de[.]com	Type squatter domain	Type squatted domain, "o" is replaced by a "0" for zepode.com. Developer of the SBS billing software.
bangladesh-bank[.]com	Domain	Bank of Bangladesh domain with the wrong top level domain. It should be .org and not .com
SBS_Billing_account_form.zip	File name	SBS is the billing software developed by zepode Inc.
Islami_Bank_KYC.zip	File name	Another reference to the Islami Bank
bracbank[.]info	Domain	A site pretending to be Brac Bank, a Bangladeshi bank. The real URL is bracbank[.]com

The campaign is believed to be a hybrid one as both Windows and Android version of the malware resorts to the same C2 hostname and port.

Popular Windows malware LodaRAT is found to be targeting Android users in Bangladesh. It was previously dubbed as "Gaza007". According to Cisco Talos Intelligence Group, a new tool Loda4Android is being used for financial gain by "Kasablanca" group. The campaign is believed to be a hybrid one as both Windows and Android version of the malware resorts to the same C2 hostname and port. The C2 for Android is being changed recently from info.v-pn[.]co to lap-top[.]xyz. The Android samples found are based on a base package of legitimate Google Play Store app named "AL-Furqan.Academy_v1.0" which belongs to an Egyptian-based Islamic college. Other than regular RAT behaviour, the sample also includes a built-in Facebook phishing kit.

Flaws in SHAREit

Source: https://www.trendmicro.com/



Trend Micro has recently released a list of vulnerabilities found in one of the most popular file sharing apps called SHAREit with over 1 billion downloads. The app contains a broadcast component which can be invoked by any app installed in the device and it can reveal SHAREit's internal and external app activities. The app contains a hidden FileProvider which leads to temporary read/ write access gain to the content provider's data and also specified root storage path can be easily accessed. Existing files in the SHAREit app can be overwritten and arbitrary code can also be executed. By exploiting deep-link feature in SHAREit app, any apk can be downloaded and installed in the device. Users are advised to update the app via Google Play Store.

Telegram Triangulation Pinpoints Users' Exact Locations

Source: https://threatpost.com/

The "People Nearby" feature in Telegram allows its users to see who's nearby and this feature could be misused to pinpoint one's exact distance from other users by spoofing one's latitude and longitude. The "People Nearby" feature could allow an attacker to triangulate the location of unsuspecting Telegram users. The feature is disabled by default, but users who enable this feature are not aware that they are publishing their exact location. It is possible to spoof one's location for three different points, and then use the resulting three distances to precisely pinpoint the target.

NCIIPC Initiatives

NCIIPC on 'March for Secure Code'

Dr. Ajeet Bajpai, DG, NCIIPC delivered Keynote Address at 'March for Secure Code' inaugural event. This platform aims to encourage thousands of students to contribute to nation building by securing cyber space. 'March for Secure Code' is a month-long programme on secure application coding and cybersecurity in partnership with NASSCOM, consisting of well-crafted course and a 'Grand challenge' for college students. Other eminent speakers were Mrs Kirti Seth, Co-Architect & Head, FutureSkills Prime and Mr. Pradeep P, Commissioner, Department of Collegiate Education, Government of Karnataka.

NCIIPC on India Future Foundation Seminar

Participants of India Future Foundation Seminar

India Future Foundation (IFF) in collaboration with the office of National Cyber Security Coordinator, Government of India, organised a seminar on 12th March 2021. Sh. Tathagata Datta, , NCIIPC was speaker during panel discussions on 'Securing Critical Information Infrastructure from Cyber Attacks in India (Key Issues, Challenges and Solutions)'. Other eminent speakers were Mr. Brijesh Singh (Inspector General of Police, Government of Maharashtra), Dr. Shruti Mantri (Associate Director at Indian School of Business), Mr. Amit Dubey (Co-Founder, India Future Foundation) and Mr. Karthik Ranjan (Cyber Security Specialist). Emphasis was given on security orchestration and need of security by design framework.

4th Intelect Conference by IEEMA

Participants of IEEMA virtual conference

Indian Electrical and Electronics Manufacturers' Association (IEEMA) hosted web conference (Intelect 2021) on Intelligent Electricity Distribution and Consumption. It was held on 17th February 2021, over virtual platform. Sh. Tathagata Datta, Consultant, NCIIPC spoke during panel discussions on 'Cyber

IEEMA to come up with a cyber-security framework, working jointly with OEMs, Industry, MoP, CERT and NCIIPC to ensure cyber hygiene in power & utility sector

Security – The Evolving Landscape'. Other panelists were Mr. M A K P Singh, CE CEA and CISO MoP; Mr. A.P. Singh, SE IT, UPPCL; and Mr. S. Samanta, Head IT, TPDDL. Major topics discussed were:

- IEEMA to come up with cyber-security framework, working jointly with OEMs, Industry, MoP, CERT and NCIIPC to ensure cyber hygiene in power & utility sector.
- Need for better Coordination among MoP, CERT Generation, CERT Trans, CERT Distribution and NCIIPC.
- Focus on developing Threat Hunting and Incident Response Capabilities.
- Training to increase awareness among stakeholders.

Webinar Organised by Department of IT & E, Govt. Of West Bengal

Participants of West Bengal's webinar

West Bengal Electronics Industry Development Corporation (WBEIDC) Ltd., nodal agency to Department of Information Technology & Electronics, Government of West Bengal, organised webinar, titled "Leveraging Innovation & Business Growth through Emerging Technologies" on 28th January 2021 to promote and create awareness on the emerging technologies. Dr. Piyush Sharma, Director, NCIIPC Zonal Centre (East) participated in the webinar to discuss 'Importance of Cyber Security and Data security in our personal & professional life- recent trends'.

Seminar on Data Protection and Policy Framework in India

Participants of the web-seminar

Web-seminar on 'Data Protection and Policy Framework in India' was organised by leading cyber security forum InfoSec Foundation on 6th March 2021. NCIIPC emphasised on the relevance of Zero Trust Framework in current context and also explained how it is assisting critical sector organisations to align their risk assessment with a framework to ensure consistency in meeting cyber security objectives and protect national interest. Other eminent speakers in the web-seminar were Mr. Pavan Duggal, Advocate Supreme Court; Mr. Rajeev Kumar (IPS), Principle Secretary IT & E, Government of WB; Mr. Sanjay Kr Das, Jt Secretary IT & E. Government of WB; and Mr. Arnab Neogi, Head IT, Tata Medical Cancer Hospital.

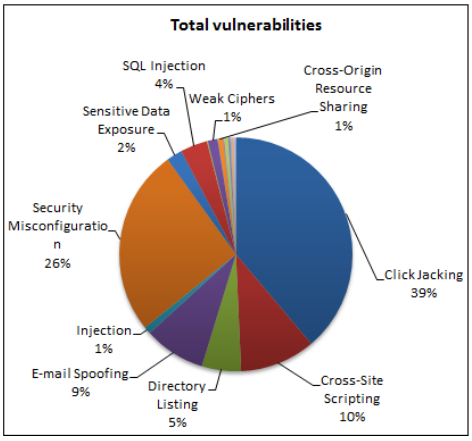
NCIIPC Responsible Vulnerability Disclosure Program

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. There are 1750 vulnerabilities reported during the first quarter of 2021. The top 10 vulnerabilities are:

- Click Jacking

- Security Misconfiguration
- Cross-Site Scripting
- E-mail Spoofing
- Directory Listing
- SQL Injection
- Sensitive Data Exposure
- Weak Ciphers
- Injection
- Cross-Origin Resource Sharing



Around 239 researchers participated in RVDP programme during the first quarter of 2021. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Aakash Madaan
- Gulshan Kumar
- Harshal S. Sharma
- Kunal Narsale
- Nikhil Kumar
- Parshwa Bhavsar
- Parth Surati
- Prathamesh Surekha Prakash Pawar
- Rahul Parmar
- Ratnadip Gajbhiye
- Sai Manikanta Teja Parwatha
- Santosh Kumar Sha
- Securium Solutions Pvt Ltd
- Shashwat
- Vivek Panday

APRIL 2021

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

MAY 2021

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

Upcoming Events - Global

April 2021

- SANS Cyber Security Mountain: April 2021, Virtual 5-10 Apr
- CRESTCon Australia 2021, Virtual 8 Apr
- SecureWorld Mid-Atlantic Virtual Conference, Virtual 8 Apr
- Cybersecurity Summit ANZ, Virtual 13-14 Apr
- BSides Cape Girardeau, Virtual 17 Apr
- Cybersecurity & Fraud Summit: Mid-West, Virtual 27-28 Apr
- BSides Oklahoma, Virtual 28-30 Apr
- FutureCon San Antonio CyberSecurity Conference, Virtual 29 Apr
- Phoenix Portland Virtual Cybersecurity Conference, Virtual 29 Apr

May 2021

- SANS Cyber Security Central: May 2021, Virtual 3-8 May
- Cybersecurity Summit: Pacific North-West, Virtual 4-5 May
- CyFrica 2021, Virtual 4-5 May
- Black Hat Asia, Virtual 4-7 May
- Cyber Security for Critical Assets (CS4CA) World Summit 2021, Virtual 6 May
- CyberCon London 2021, Virtual 12-13 May
- FutureCon Toronto CyberSecurity Conference, Virtual 13 May
- RSA Conference USA 2021, Virtual 17-20 May
- Data Connectors Northern California Virtual Cybersecurity Summit, Virtual 25 May

June 2021

- ManuSec Europe, Virtual 1-2 Jun
- Cyberx Qatar 2021, Virtual 7-8 Jun
- The 3rd ACM International Symposium on Blockchain and Secure Critical Infrastructure, Hong Kong 7-11 Jun
- Cybersecurity Summit: North-East, Virtual 8-9 Jun
- InfoSecurity Europe 2021, Virtual 8-10 Jun
- Florida Caribbean Virtual Cybersecurity Conference, Virtual 16 Jun
- Cybersecurity Summit: Canada, Virtual 22-23 Jun
- Interface Phoenix 2021, Virtual 24 Jun

July 2021

- 18th International Conference on Security and Cryptography (SECRYPT), Virtual — 6-8 Jul
- St. Louis/OKC Cyber Security Summit, Virtual — 7 Jul
- 5th International Symposium on Cyber Security Cryptology and Machine Learning, Virtual — 8-9 Jul
- Blockchain and Internet of Things Conference (BIOTC), Ho Chi Minh City — 8-10 Jul
- International Workshop on Cryptography, Security and Privacy (IWCSP), Budapest — 9-11 Jul
- Detroit Cyber Security Summit 2021, Virtual — 14 Jul
- The 7th International Conference on Artificial Intelligence and Security (ICAIS), Dublin — 19-23 Jul
- Black Hat USA 2021, Las Vegas — 31 Jul-5 Aug

JUNE 2021

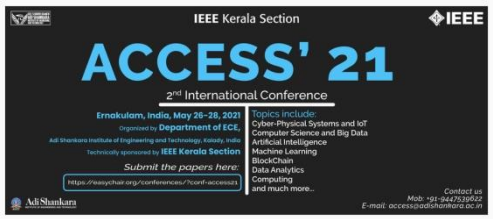
S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Upcoming Events - India

- The International Conference on Cyber Security and Digital Forensics, Virtual — 3-4 Apr
- International Conference on Emerging Electrical Systems and Control (ICEESC), Virudhunagar — 9-10 Apr
- 2nd International Conference on Future Communication & Computing Technology (ICFCCT), Mumbai — 29-30 Apr
- Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), Virtual — 11-14 May
- 2nd International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS), Kalady — 26-28 May

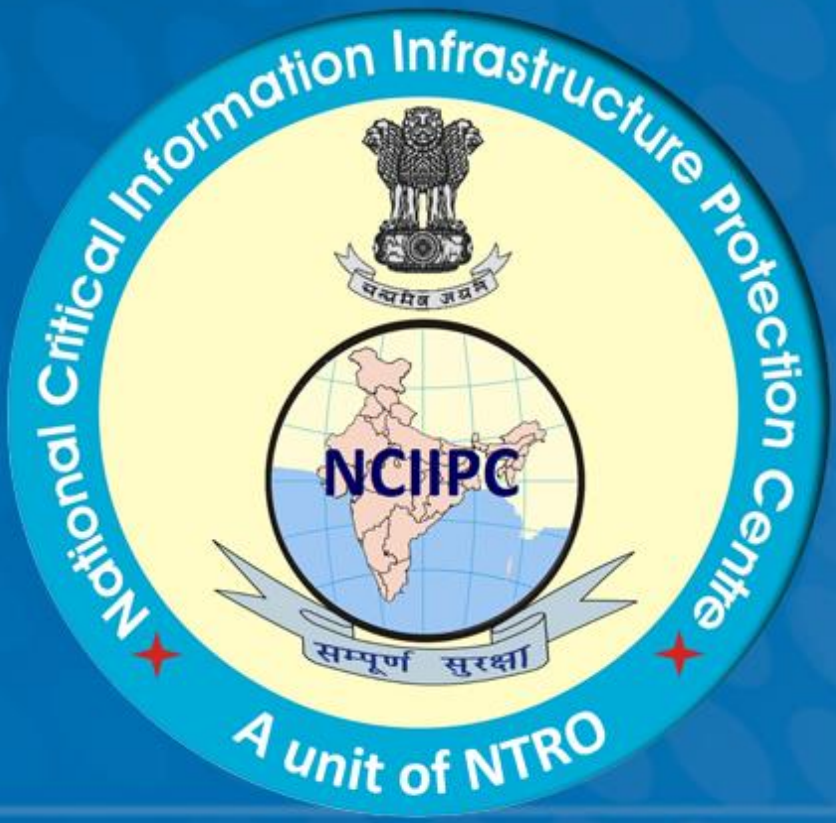
JULY 2021

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



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

Notes



Feedback/Contribution

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

Copyright
NCIIPC, Government of India

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.