NEWSLETTER

January 2022

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

Celebrating 8th Foundation Day

16th January 2014

NCIIPC is the National Nodal Agency created under Section 70A of the IT Act, 2000 (amended 2008), in respect of CII Protection

Vision

"To facilitate safe, secure and resilient Information Infrastructure for Critical Sectors of the Nation."

Mission

"To take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders."

Critical Sectors

POWER & ENERGY

GOVERNMENT

TRANSPORT

TELECOM

BANKING, FINANCE & INSURANCE

STRATEGIC & PUBLIC ENTERPRISES

Facilitating Protection of Nation's CII & Raising Information Security Awareness among Stakeholders through :

CII Identification

Security Assessment

Malware Reporting

Vulnerability Assessment

Threat Assessment

Incident Reporting

Knowledge Management System

Responsible Vulnerability Disclosure Program

Protection from Social Engineering Attacks

Risk Assessment

Vulnerability Reporting

Cyber Security Audit

https://nciipc.gov.in/

@NCIIPC

NCIIPC India

NCIIPC India

helpdesk1@nciipc.gov.in

VOLUME 6 ISSUE 1

@NCIIPC

NCIIPC Newsletter

January 2022

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

NCIIPC celebrates its 8th foundation day on this 16th January 2022. It was the day when Govt. of India declared NCIIPC as National Nodal Agency for protection of Critical Information Infrastructure (CII) through a Gazette Notification. The NCIIPC has gone a long way in these years to take steps for identification and protection of National Critical Information Infrastructures. The NCIIPC Responsible Vulnerability Disclosure Program has seen a big rise in reporting and patching of vulnerabilities related to CIIs.

There is increased awareness among critical sector organisations for implementing best practices towards security of CII. The cyber threat landscape has also increased manifold in these years. Ransomware, Ransomware-as-a-Service, Crypto Mining, Phishing Attacks, Fileless Malware and various new advanced techniques have emerged in these years. NCIIPC has established and expanded National Security Analysis Centre to continuously monitor the security stance of CII organisations. Any threats or breaches are proactively and timely detected and reported to CII stakeholders. NCIIPC is continuously evolving its Threat Assessment Framework in order to timely identify and reporting of the emerging threats to its stakeholders.

NCIIPC celebrated National Cyber Security Awareness month October 2021. NCIIPC conducted various webinars and cyber security awareness programs in partnership with industry and CII stakeholders to create awareness and cyber security strategy for our nation.

NCIIPC wishes a happy and safe new year for all its readers and stakeholders. We recommend adopting safe practices to protect from new variants of Corona virus as per the guidelines issued by Ministry of Health and Family Welfare.

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

Quad Countries Announce Shared Cyber Standards

Source: https://www.whitehouse.gov/, https://www.zdnet.com/

The Quadrilateral Security Dialogue, known as the Quad comprising of India, Japan, Australia, and United States, announced to develop new global cybersecurity standards across various technology sectors to make cyberspace and emerging critical technologies trusted and secure. Also, a new Quad Senior Cyber Group would be established. This group would consist "leader-level experts" who would meet regularly to advance work between government and industry. This would drive the adoption and implementation of shared cyber standards, secure software development, tech workforce growth, and promotion of scalability and cybersecurity of secure and trustworthy digital infrastructure. The security bloc would begin cooperation focused on combatting cyber threats, promoting resilience, and securing critical infrastructure together.

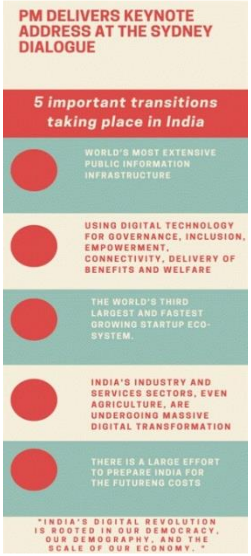
The Quadrilateral Security Dialogue

The security bloc would begin cooperation focused on combatting cyber threats, promoting resilience, and securing critical infrastructure together.

PM Modi Delivered Keynote Address at The Sydney Dialogue

Source: https://pib.gov.in/Pressreleaseshare.aspx?PRID=1772806

On 18 November 2021, honourable Prime Minister Sh. Narendra Modi delivered the keynote address at The Sydney Dialogue, an initiative of the Australian Strategic Policy Institute. He spoke on the theme of India's technology evolution and revolution. Sh. Narendra Modi stated India's central role in the Indo Pacific region and in the emerging digital world. He said, "India's digital revolution is rooted in our democracy, our demography, and the scale of our economy. It is powered by enterprise and innovation of our youth. We are turning the challenges of the past into an opportunity to take a leap into the future". He also added that India is now committed towards data protection, privacy and security, and use data as a source of empowerment of people.



PM DELIVERS KEYNOTE ADDRESS AT THE SYDNEY DIALOGUE

5 important transitions taking place in India

- WORLD'S MOST EXTENSIVE PUBLIC INFORMATION INFRASTRUCTURE
- USING DIGITAL TECHNOLOGY FOR GOVERNANCE, INCLUSION, EMPOWERMENT, CONNECTIVITY, DELIVERY OF BENEFITS AND WELFARE
- THE WORLD'S THIRD LARGEST AND FASTEST GROWING STARTUP ECO-SYSTEM.
- INDIA'S INDUSTRY AND SERVICES SECTORS, EVEN AGRICULTURE, ARE UNDERGOING MASSIVE DIGITAL TRANSFORMATION
- THERE IS A LARGE EFFORT TO PREPARE INDIA FOR THE FUTURENG COSTS

"INDIA'S DIGITAL REVOLUTION IS ROOTED IN OUR DEMOCRACY, OUR DEMOGRAPHY, AND THE SCALE OF OUR ECONOMY. "

Odisha Establishes Cyber Security Operation Centre

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

The government of Odisha has taken a significant step towards cyber security and has established a mechanism to protect its websites and applications from hackers. A Cyber Security Operation Centre (CSOC), to prevent any cyber intrusion and defacement attempts, is being built on the premises of the

ocac

Odisha Computer Application Centre

Image source: https://www.ocac.in/

Odisha Computer Application Centre (OCAC) tower. The objective of the CSOC would be to monitor suspicious inbound traffic and would take immediate preventive measures against malicious users. The role of CSOC would be to monitor, detect, investigate and respond to cyber threats. The CSOC would study each threat minutely, discard the false ones and ascertain real threats.

India-ITU Joint Cyberdrill 2021

Source: https://telecom.economictimes.indiatimes.com/, https://www.itu.int/

The Department of Telecommunications (DoT) and the International Telecommunication Union (ITU), a United Nations (UN) agency, held the India-ITU Joint Cyberdrill 2021. India-ITU Joint Cyberdrill 2021 is a cybersecurity exercise intended to test an organisation's capabilities to thwart or minimise the impact of cyberattack. The inaugural session was attended by more than 400 participants from sectors such as finance, power, insurance, CERT-In and CSIRT, telecom service providers, and others. This four-day virtual event was held from November 30 to December 3, 2021. The 2021 India-ITU joint CyberDrill for Indian entities emphasised the role of national Computer Incident and Response Teams (CIRTs) and Computer Security Incident Response Teams (CSIRTs) in building cyber resilience and protecting Critical Information Infrastructure.

Cyberattack Campaign Targeted Indian Government & Military

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

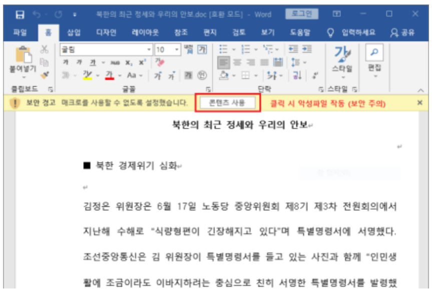
Cisco Talos discovered a cyber-attack campaign, named 'Armor Piercer', that targeted Indian military personnel and government employees. This campaign disseminates malicious documents to deliver Remote Access Trojans and gain access to highly confidential information related to defence and government agencies. This campaign used the operational documents of 'Kavach', a two-factor authentication app by National Informatics Centre and used by government employees to access their emails. This campaign used maldocs, a malicious MS Office document, disguised as software installation guides, security advisories or meeting schedules, etc. It was also discovered that this campaign used various techniques and evolved to obfuscate itself in order to remain in the victim's environment by evading standard detection techniques.

News Snippets - International

Social Media Platform Used to Launch a Cyber Attack

Source: https://www.dailynk.com/

Recently, a hacker group known as Kumsong 121 used an elaborate method of social media to launch a cyber- attack. EST Security observed this Advanced Persistent Threat (APT) by Kumsong 121. This APT used social media to befriend the target and sent an infected file. It hacked an individual's social media account and then attackers chose additional targets from the victim's social media friends. The hackers lowered the targets guard and earned their friendship. Then send an infected document file to the target through email. The attached document file contains a macro virus that renders the target's computer hackable if the email recipient approves the file.



보안 경고 매크로를 사용할 수 없도록 설정했습니다. 콘텐츠 사용 클릭 시 악성파일 작동 (보안 주의)

북한의 최근 정세와 우리의 안보

■ 북한 경제위기 심화

김정은 위원장은 6월 17일 노동당 중앙위원회 제8기 제3차 전원회의에서 지난해 수해로 "식량형편이 긴장해지고 있다"며 특별명령서에 서명했다. 조선중앙통신은 김 위원장이 특별명령서를 들고 있는 사진과 함께 "인민생활에 조금이라도 이바지하려는 충심으로 친히 서명한 특별명령서를 발령했

A document with malicious code recently distributed by hackers
Image: EST Security Response Centre

Hackers Compromised Servers of Indonesian Govt. Agencies

Source: https://therecord.media/, https://kr-asia.com/

Insikt Group researchers discovered intrusions, suspected to be linked to a hacker group called Mustang Panda, in the internal networks of ten of Indonesia's government organisations in April 2021. The Insikt researchers discovered PlugX malware command and control (C&C) servers, operated by the Mustang Panda group, communicating with hosts inside the networks of the Indonesian government. The point of intrusion and the delivery method of the malware are unclear. These intrusions were notified to the Indonesian authorities in June and again in July 2021. However, the authorities took steps to identify and cleanse the infected systems in August 2021. Later, the Insikt researchers confirmed that hosts inside Indonesian government networks were still communicating with the Mustang Panda malware servers.

Insikt Group

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

Later, the Insikt researchers confirmed that hosts inside Indonesian government networks were still communicating with the Mustang Panda malware servers.

Giant Israel Communications Firm Hit by Major Cyberattack

Source: https://www.middleeastmonitor.com/

A major cyberattack hit Israeli's giant communications firm Voicenter on 18 September 2021. The cyberattack was carried out by a group of hackers from abroad. This cyberattack paralysed the communication systems of a number of firms that received services from Voicenter. It was also found that a hacker named Deus managed to steal 15 terabytes of data from the company and put up for sale. Voicenter CEO Golan Ashtan confirmed that hackers launched a cyberattack on Voicenter's systems, but also claimed that no sensitive information were leaked.

VOICENTER

Image source: https://www.voicenter.co.il/

CEO Andrew Bills stated that the ransomware attack was attack was contained by segregating the corporate network from other internal networks and enacting business continuity processes.

CS Energy Hit by Ransomware

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

CS Energy, a Queensland government-owned energy generator company, was hit by ransomware attack. CS Energy CEO Andrew Bills said that the relevant state and federal agencies were immediately notified, and they worked closely with the cybersecurity experts to resolve the matter. CEO Andrew Bills also stated that the ransomware attack was contained by segregating the corporate network from other internal networks and enacting business continuity processes. The company said that the incident had not impacted the electricity generation at Callide and Kogan Creek power station.

Image source: https://www.vestas.com/en

Wind Turbine Giant Hit by Cyberattack

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

Vestas, a Danish wind turbine giant, was hit by cyberattack on 19 November 2021. The company was forced to go offline by shutting down IT systems across multiple business units and locations to prevent the attack's spread. This cyberattack resulted in getting Vestas' data compromised. Later Vestas systems were restored and it was found that the wind turbine operations were not impacted, that suggested that the attackers did not make it through to OT systems.

Trends

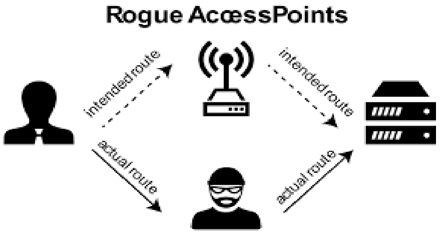


Image source: https://encrypted-tbn0.gstatic.com/

Tricking Users into Connecting to Rogue Wi-Fi Access Points

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

A new method, dubbed SSID Stripping, has been identified by a team of researchers that affects devices running Windows, macOS, Ubuntu, Android and iOS. It has been discovered that the malicious actors can manipulate the name of a wireless network, specifically the SSID (Service Set Identifier) so that it's displayed to the user with the name of a legitimate network. They are able to generate three types of 'display errors' such as implanting a NULL byte into the SSID causing Apple devices to display only the part of the name that is before this byte, the second type of display error involves using non-printable characters to the SSID that will be included in the name but will not actually be shown to the user and the third type of display error involves pushing out a certain part of the network name from the visible portion of the screen. In an SSID Stripping attack, the users see a connection whose name seems to be legitimate, but they have to manually connect to it for the attack to work. On the flip side, this bypasses the security controls since the device processes the actual string of the SSID that the malicious

In an SSID Stripping attack, the users see a connection whose name seems to be legitimate, but they have to manually connect to it for the attack to work.

actor has entered, not what the victim sees on the screen and does not stop the victim from connecting to the rogue AP.

New Gummy Browsers Attack lets Hackers Spoof Tracking Profiles

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

The 'Gummy Browsers' attack is the process of catching a person's fingerprint by making them traverse a hacker-controlled website and then using that captured fingerprint on a target platform to spoof that person's identity. Digital fingerprints are unique online identifiers linked with a specific user based on a combination of a device's characteristics and sold on dark web marketplaces, allowing malicious actors and scammers to spoof users' online fingerprints to conduct ad-fraud. There are different spoofing methods such as Script injection, Browser setting and debugging tool, and Script modification by which the user can be spoofed. Gummy Browsers can effectively impersonate the victim's browser transparently almost all the time without affecting the tracking of genuine users. The hackers can simply use the Gummy Browsers attack to trick systems using fingerprinting. The attack can spoof a user's identity to make a script seem like a human rather than a bot and be served targeted ads to perform ad-fraud and also help bypass security controls used to detect legitimate users in authentication services.

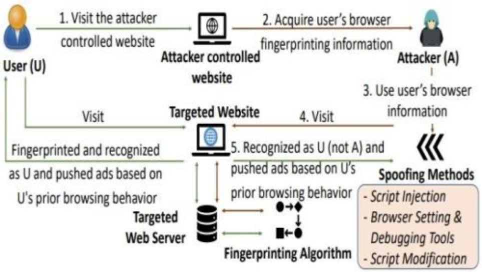

1. Visit the attacker controlled website
Attacker controlled website
2. Acquire user's browser fingerprinting information
User (U)
Attacker (A)
3. Use user's browser information
Visit
Targeted Website
4. Visit
Fingerprinted and recognized as U and pushed ads based on U's prior browsing behavior
5. Recognized as U (not A) and pushed ads based on U's prior browsing behavior
Spoofing Methods
- Script Injection
- Browser Setting & Debugging Tools
- Script Modification
Targeted Web Server
Fingerprinting Algorithm

Image source: https://i0.wp.com/www.bleepstatic.com/

The hackers can simply use the Gummy Browsers attack to trick systems using fingerprinting.

Google Spots Technique to Sneak Malware Past Detection Tools

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

A new technique has been used by a financially motivated attacker to sneak adware and other malware past security tools. It has been discovered that the threat actor is using a software code-signing certificate from a legitimate certificate authority to create signatures that can't be parsed or decoded by security products that use OpenSSL code but are accepted as valid by Windows. This threat actor has been using these signatures to distribute a known malware family i.e OpenSUpdater which is used to install other unwanted and potentially harmful software on infected systems. Threat Actors have used stolen or else illegally obtained digital certificates to bypass malware detection tools and extend the ability of their malware to stay hidden on compromised systems and networks. Groups of OpenSUpdater samples have been observed to be signed with a deliberately malformed signature to evade detection.

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

Groups of OpenSUpdater samples have been observed to be signed with a deliberately malformed signature to evade detection.

New Technique Lets Hackers Hide Vulnerabilities in Source Code

Source: https://thehackernews.com/

Trojan Source attacks, a technique that has been used by threat actors to exploit a novel class of vulnerabilities by injecting visually deceptive malware in a way that's semantically permissible but alters the logic defined by the source code, successfully opening the door to more first-party and supply chain risks. This technique abuses subtle ties in text-encoding standards such as Unicode to produce source code whose tokens are logically coded in a different order from the one in which they are displayed, leading to vulnerabilities that cannot be perceived directly by human code reviewers. The novel class of vulnerabilities tracked as CVE-2021-42694 and CVE-2021-42574 affect programming languages such as C, C++, Java, C#, Rust, Python, and JavaScript. Trojan Source attack creates discrepancies by inserting Unicode Bidi override characters into comments and strings that yield syntactically-valid source code in which the display order of characters presents logic that diverges from the actual logic.

Trojan Source attack creates discrepancies by inserting Unicode Bidi override characters into comments and strings that yield syntactically-valid source code in which the display order of characters presents logic that diverges from the actual logic.

Phishing-as-a-Service is Responsible for Many Business Attacks

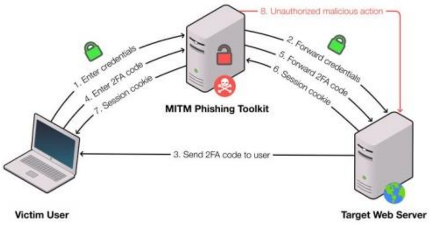
Source: https://www.zdnet.com/

The Phishing-as-a-Service operation involves selling fake login pages for cloud services like OneDrive that help non-technical threat actors steal business user passwords and usernames. This full-scale phishing facilitator offers more than 100 phishing templates that impersonate big brands and services and is responsible for many of the phishing campaigns that hit companies. This phishing-as-a-service business provides email and website templates as phishing kits do, but also offers email delivery, hosting services, credential theft, fully undetected (FUD) links and logs for buying as a weekly, fortnightly, monthly, or annual subscription. These service providers host the pages and links and cybercriminals who pay for these services simply obtain the stolen credentials later on. These businesses caught the attention of security experts as they offer dozens of login scam templates for Microsoft OneDrive, LinkedIn, Adobe, Alibaba, American Express, AOL, AT&T, Dropbox, and Google Docs. It allows anyone on a small budget to beat a path to theft or extortion.

This phishing-as-a-service business provides email and website templates as phishing kits do, but also offers email delivery, hosting services, credential theft, fully undetected (FUD) links and logs for buying as a weekly, fortnightly, monthly, or annual subscription.

New Way to Detect MitM Phishing Kits in the Wild

Source: https://thehackernews.com/



A MitM phishing toolkit empowers fraudsters to sit between a victim and an online service. Rather than setting up a bogus website that's circulated via spam emails, the threat actors deploy a fake website that mirrors the live content of the target website and acts as a channel to forward requests and responses between the two parties in real-time, thus permitting the extraction of credentials and session cookies from 2FAauthenticated accounts. They function as reverse proxy servers, brokering communication between victim users and target web servers, all while collecting sensitive information from the network data in transit. A new fingerprinting method has been formulated by the researchers that include an ML classifier using network-level features such as TLS fingerprints and network timing discrepancies to categorise phishing websites hosted by MitM phishing toolkits on reverse proxy servers. It also involves a data-gathering framework that monitors and crawls suspicious URLs from open-source phishing databases like PhishTank and OpenPhish, among others. The main idea is to measure the Round-Trip Time (RTT) deferrals that arise out of employing a MitM phishing kit, which, in turn, surges the duration from when the victim browser sends a request to when it receives a response from the target server due to the fact that the reverse proxy intermediates the communication sessions. PHOCA, named after the Latin word for seals, the tool not only enables the discovery of previously unseen MitM phishing toolkits but also can be used to spot and separate malicious requests coming from such servers, can be directly incorporated into current web infrastructure such as phishing blocklist services to expand their coverage on MitM phishing toolkits.

The threat group is typically targeting publicly facing web servers to install web shells for initial intrusion and then further scatters inside the network.

Malware Bytes

Spy Group 'Grayfly' Uses Sidewalk Malware

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

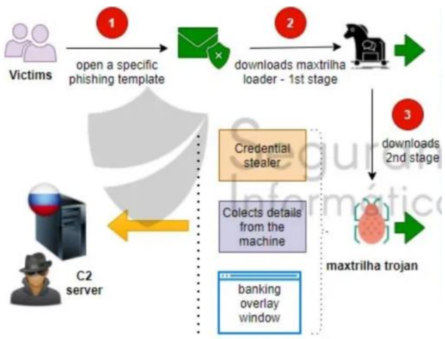
The recent threat campaign by spy group 'Grayfly' is using SideWalk malware to target victim systems. The threat campaign is targeting a number of countries in Europe, Asia, and North America across a variety of industries, including financial, healthcare, hospitality, manufacturing, food and telecommunications. The threat group is typically targeting publicly facing web servers to install web shells for initial intrusion and then further scatters inside the network. Grayfly may install its custom backdoors onto additional systems after compromising the network. After the installation of backdoor, the attackers deployed a custom version of the credential-dumping tool Mimikatz.

The threat group is typically targeting publicly facing web servers to install web shells for initial intrusion and then further scatters inside the network.

New Maxtrilha Trojan Disseminated and Targeting Several Banks

Source: https://securityaffairs.co/

A new banking trojan, Maxtrilha has been targeting several banks around the world. According to the targeted countries, the campaign has been leveraged by Brazilian threat group gangue. Threat group uses customised phishing templates to spread the trojan Maxtrilha. At the initial stage, the loader opens a legitimate


1
Victims
open a specific phishing template
2
downloads maxtrilha loader - 1st stage
3
downloads 2nd stage
Credential stealer
Colects details from the machine
banking overlay window
maxtrilha trojan
C2 server

service presented on the phishing template to lure victims during its execution. The 1st stage creates persistence on the infected system, disables Internet Explorer security settings and accepted extensions to facilitate the download of the 2nd stage. The 2nd stage checks or creates persistence on the machine, installs or modifies Windows trusted certificates, checks by opening windows to perform banking windows overlay to steal credentials and can deploy additional payloads executed via DLL injection technique. The victims' data is encrypted and sent to the Command & Control (C2) server.

Drinik Malware Fooling Users to Give Their Mobile Banking Details

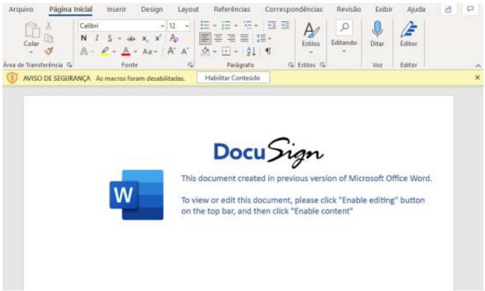
Source: https://www.itsecuritynews.info/

The Drinik malware is observed being imitating a legitimate version of Income Tax Department's solution for generating tax refunds.

Drinik malware is stealing vital data and financial credentials from smartphone users. The Drinik malware is observed being imitating a legitimate version of Income Tax Department's solution for generating tax refunds. After a user has been duped into downloading it, all sensitive data will be collected. It requests for authorisation to view SMS messages, phone records, and contacts, as well as a refund application form seeking information like as full name, PAN, Aadhaar number, address, and date of birth. All sensitive banking information such as account number, IFSC code, CIF number, debit card number, expiration date, CVV, and PIN is requested. The malware also forces the user to complete a transaction.

Squirrelwaffle: A New Malware Loader

Source: https://cyware.com/



AVISO DE SEGURANÇA As macros foram desabilitadas.

This document created in previous version of Microsoft Office Word.

To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"

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

Threat actors are using new malware loader Squirrelwaffle, to gain an initial foothold into targeted networks and drop malware. The spam campaign mostly uses stolen reply-chain email campaigns and the DocuSign signing platform as a lure to fool victim into enabling macros on their MS Office suite. Previously compromised web servers are being used to support the file distribution action, where most of the sites are running WordPress 5.8.1 version. Squirrelwaffle deploys malware such as Qakbot or Cobalt Strike in post exploitation. All communications between Squirrelwaffle and its Command & Control (C2) communications are encrypted and sent using HTTP POST requests.

Clop Gang Exploiting SolarWinds Serv-U Flaw

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

The Clop ransomware gang, also tracked as FIN11 and TA505, is observed being exploiting SolarWinds Serv-U vulnerability to breach corporate networks and ultimately encrypt its devices.

The Serv-U Managed File Transfer and Serv-U Secure FTP Remote Code Execution (RCE) vulnerability (CVE-2021-35211) allows a remote threat actor to execute commands on a vulnerable server with elevated privileges. This vulnerability only affects systems with enabled SSH feature. It is also reported that TA505 more usually uses phishing emails with malicious attachments to breach networks. Another sign of exploitation is traces as PowerShell command execution used to deploy a Cobalt Strike beacon on the vulnerable system.

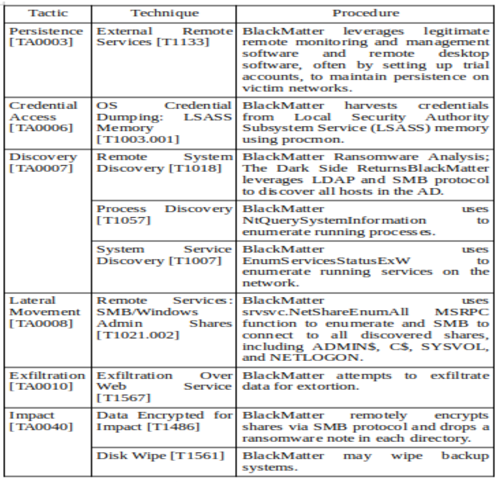
Bulletproof Hosting
Code Signing Certificates
Publicly Available Malware
Domain Registration Services
FIN11
Figure 1.
Services used by FIN11.

Image source: https://i0.wp.com/

BlackMatter Ransomware

Threat Assessment Group, NCIIPC

BlackMatter is a new threat actor (ransomware) found during July 2021. It relies on Ransomware-as-a-Service (Raas) tool. BlackMatter attacking pattern is similar to DarkSide, which was found active during September 2020 to May 2021.



Tactic	Technique	Procedure
Persistence [TA0003]	External Remote Services [T1133]	BlackMatter leverages legitimate remote monitoring and management software and remote desktop software, often by setting up trial accounts, to maintain persistence on victim networks.
Credential Access [TA0006]	OS Credential Dumping: LSASS Memory [T1003.001]	BlackMatter harvests credentials from Local Security Authority Subsystem Service (LSASS) memory using procmon.
Discovery [TA0007]	Remote System Discovery [T1018]	BlackMatter Ransomware Analysis; The Dark Side ReturnsBlackMatter leverages LDAP and SMB protocol to discover all hosts in the AD.
	Process Discovery [T1057]	BlackMatter uses NtQuerySystemInformation to enumerate running processes.
	System Service Discovery [T1007]	BlackMatter uses EnumServicesStatusExW to enumerate running services on the network.
Lateral Movement [TA0008]	Remote Services: SMB/Windows Admin Shares [T1021.002]	BlackMatter uses srvsvc.NetShareEnumAll MSRPC function to enumerate and SMB to connect to all discovered shares, including ADMIN$, C$, SYSVOL, and NETLOGON.
Exfiltration [TA0010]	Exfiltration Over Web Service [T1567]	BlackMatter attempts to exfiltrate data for extortion.
Impact [TA0040]	Data Encrypted for Impact [T1486]	BlackMatter remotely encrypts shares via SMB protocol and drops a ransomware note in each directory.
	Disk Wipe [T1561]	BlackMatter may wipe backup systems.

Tactics, Techniques, and Procedures (TTP)

Tactics, Techniques, and Procedures (TTP): The BlackMatter variant uses previously compromised admin or user credentials. BlackMatter threat actors use the embedded credentials in the Lightweight Directory Access Protocol (LDAP) and Server Message Block (SMB) protocol. This variant of BlackMatter leverages the embedded credentials and SMB protocol to encrypt remotely from the original compromised host, all discovered shares' contents, including ADMIN$, C$, SYSVOL, and NETLOGON etc. This threat actor uses an encryption binary for Linux-based machines and ESXi virtual machines separately. BlackMatter actors keep reformatting backup data stores, rather than encrypting backup systems. BlackMatter ransomware uses TTPs pattern as similar to DarkSide like Coding styles, Dynamic functions, Same compression algorithm for the configuration, Storing of the victim id

BlackMatter actors keep reformatting backup data stores, rather than encrypting backup systems.

References:

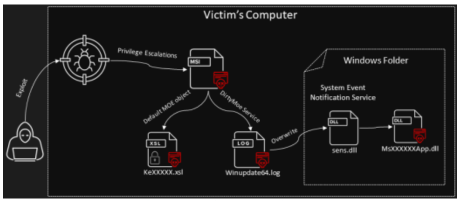
[1] https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/blackmatter-ransomware-analysis-the-dark-side-returns/

[2] https://us-cert.cisa.gov/ncas/alerts/aa21-291a

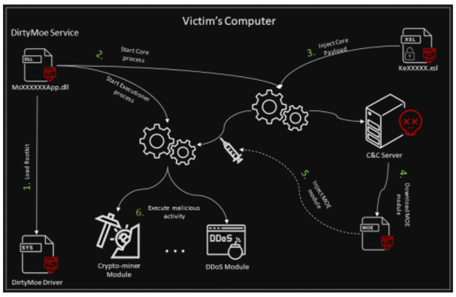
Dirty Moe Malware

Source: https://decoded.avast.io/martinchlumecky/dirtymoe

The Dirty Moe malware uses modern techniques which are modularised and spread via Cryptojacking and DDoS attacks. Dirty Moe run as a Windows service under system-level privileges via Eternal Blue and three other exploits. Dirty Moe downloads an



Kill Chain: Delivery



Kill Chain: Exploitation and Installation

encrypted payload as per target vulnerabilities and injects the payload into itself. It extracts a Windows driver that uses various rootkit specialisation like registry entry, and driver hiding. Secondly, the windows driver can hide selected files on the system data and can inject an arbitrary DLL. Dirty Moe directs a DNS request to at least one hard-coded domain using DNS servers. However, the final IP address and port are derived using another sequence of DNS requests. Hence blocking final IP address does not neutralise the malware, and DNS requests cannot block DNS server.

Reconnaissance and Execution:

- Through port-scanning and open-database of vulnerabilities, Purple Fox exploit kit is used by Dirty Moe Malware.
- Phishing emails having URLs that can exploit targets via Internet browsers like the Scripting Engine Memory Corruption Vulnerability (CVE-2020-0674) are used. When attacker gets access to administrator user login, the code takes control over the affected system.
- Dirty Moe uses Windows MSI Installer to deploy the malware which provides easy way to install software across various platforms and versions of Windows OS. The malware can easily install Dirty Moe malicious code in the targeted System.
- Registry Manipulation
- File Manipulation
- MSI Installation
- Command and Control: Dirty Moe does not use fixed IP addresses but implements a unique technique to obfuscate the final C&C server address. So, it is impossible to block the C&C server on a victim's machine as server address changes for each C&C communication.

> *Dirty Moe uses Windows MSI Installer to deploy the malware Which provides easy way to install software across various platforms and versions of Windows OS.*

Learning

Cyber Threat Intelligence (CTI) and MISP: The Additional Security Weapon for Organisations

Threat Assessment Group, NCIIPC

The procedure of defending assets from unauthorised access, disclosure, modification, inspection and destruction is as primitive as man's existence on earth. In Cybersecurity the Cyber Threat Intelligence (CTI) is the further attempts of man to continue an analogous practice by utilising the data about threats and threat actors stored in CTI to mitigate harmful events in cyberspace. CTI can enable better-informed security, business decisions and permit organisations to require decisive action to protect sensitive data against cyber threat adversaries. Threat intelligence is further categorised into three subcategories:

> *CTI can enable better-informed security, business decisions and permit organisations to require decisive action to protect sensitive data against cyber threat adversaries.*

Tactical: Technical intelligence includes IoCs such as IP addresses, domains, and hashes which can be used to help in the identification of threat actors.

Operational: Operational intelligence includes the motivation, capabilities and other operational information of threat actors along with TTPs (Tools, Techniques and Procedures).

Strategic: It deals with the overarching risks associated with cyber threats which can be applied to drive high-level organisational strategy usually meant for a non-technical audience.

Benefits of Cyber Threat Intelligence:

- Enables improved detection of threats.
- Enables sharing of intelligence and experiences within the cyber security community and stakeholders.
- Superior decision-making before, during and after the detection of an incident.
- Provide IoCs for computer emergency response teams and incident response groups.

Operational intelligence includes the motivation, capabilities and other operational information of threat actors along with TTPs (tools, techniques and procedures).

Developed by the developers from CIRCL, Belgian Defence, NATO, and NCIRC, Malware Information Sharing Platform (MISP) is a free and open-source platform that allows sharing, storing, and correlating of Indicators of Compromise (IoCs) of targeted attacks, threat intelligence, vulnerability intelligence etc. In the field of Cybersecurity information sharing is key element in detecting security breaches and proactively protecting information systems and infrastructures.

It enables in-built sharing functionality by using various models of distributions and also automatically synchronise events with their attributes. It has filtering functionality that can be utilised to meet an organisation's sharing policy. By using the user interface of MISP; end-users can create and collaborate on events, attributes, and Indicators of Compromise (IoCs). MISP come up with facility to ingest and analyse threat data on detected malware attacks, automatically creating connections between malware and their characteristics, and storing data in a structured format which helps the security analysts.

MISP come up with facility to ingest and analyse threat data on detected malware attacks, automatically creating connections between malware and their characteristics, and storing data in a structured format which helps the security analysts.

Features of MISP as a CTI:

- It enables efficient management of IoCs in a centralised space and also permits to store technical, non-technical information about malware samples, incidents, attackers and intelligence.
- It supports flexible sharing groups, automatic correlation of indicators, free text import, event distribution and collaboration.
- A user friendly interface for end-user to create, update and collaborate on events and indicators.
- Easy integration with security infrastructure (REST API).

- Email alerting.
- Data can be exported in the STIX format (XML and JSON) including STIX 2.0 (import/export) format.
- It supports API integration with PyMISP which is very helpful to fetch, add or update events attributes, handle malware samples and search for attributes.

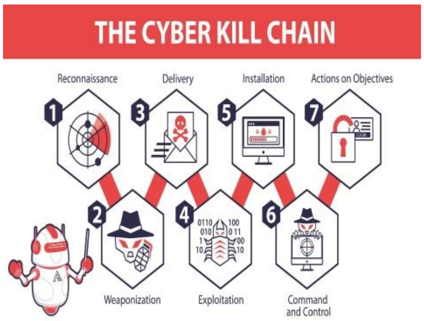
It supports API integration with PyMISP which is very helpful to fetch, add or update events attributes, handle malware samples and search for attributes.

References:

[1] https://cyware.com/educational-guides/cyber-threat-intelligence/what-is-malware-information-sharing-platform-misp-b28e

[2] https://www.misp-project.org/features.html

[3] https://en.wikipedia.org/wiki/Malware_Information_Sharing_Platform



Understanding Cyber Kill Chain

Threat Assessment Team, NCIIPC

The cyber kill chain is a sequence of steps that tracks down stages of a cyberattack from the initial reconnaissance phase to the exfiltration of data. This cyber kill chain model is created by Lockheed Martin that helps us understand and combat ransomware, security breaches, identify vulnerabilities, Advanced Persistent Attacks (APTs) and helps security teams to terminate the attacks at every stage of the kill chain. The term kill chain is obtained from the military, which uses this term related to the structure of an attack. It consists of target identification, dispatch, decision, order, and at last destruction of the target. How does the Cyber Kill Chain Work? The cyber kill chain consists of 7 well defined steps:

The cyber attacker collects data about the target and the tactics for the attack which includes harvesting email addresses and collecting other information about network, tools, devices protocols and critical infrastructure.

Reconnaissance: The cyber attacker collects data about the target and the tactics for the attack which includes harvesting email addresses and collecting other information about network, tools, devices protocols and critical infrastructure. Automated scanners are being used by threat actors to find vulnerabilities in the system by scanning firewalls, intrusion prevention systems etc. to get a point of entry for the cyber-attack. There are two types of reconnaissance attack: Passive reconnaissance and Active reconnaissance

Weaponisation: Threat actors develop malware by leveraging security vulnerabilities. Cyber attackers develop malware based on their needs and intention of the attack. This phase also involves attackers trying to reduce the chances of getting detected by the security solutions that the critical organisation has set up.

Delivery: The weaponised malware is delivered by cyber attackers via a phishing email or some other medium. The most common methods for delivering weaponised payloads include websites, removable disks, and emails. This is the most important phase of cyber kill chain where the attack can be stopped by the security teams.

The weaponised malware is delivered by cyber attackers via a phishing email or some other medium. The most common methods for delivering weaponised payloads include websites, removable disks, and emails.

Exploitation: The malicious code is delivered into the organisation's infrastructure by breaching the perimeter and with this an attacker gets the opportunity to exploit the organisation's systems by installing tools, running scripts, and modifying security certificates. In most cases an application or the operating system's vulnerabilities are targeted. Scripting, dynamic data exchange, and local job scheduling are few examples of exploitation attacks.

Installation: A backdoor or remote access trojan is installed by the malware that provides access to the attacker. This is again an important stage of cyber kill chain where the attack can be stopped using systems such as HIPS (Host-based Intrusion Prevention System).

Command and Control: The attacker gets control over the organisation's systems and network. Threat actors attempt brute force attacks, look for credentials, gain access to privileged accounts and change permissions to take over the control of the system. This phase also allows the attacker to move deeper into the network, conduct destruction or denial of service operations and exfiltrate data.

The attacker gets control over the organisation's systems and network.

Actions on Objective: The attacker finally exfiltrate the data from the system. The objective of this step involves gathering, encrypting, and exfiltrating confidential information from the organisation's infrastructure, violations of data integrity or availability are potential objectives as well.

Leaving cybersecurity vulnerabilities open for security attacks is one of the most common mistakes made by critical organisations today. Continuous security validation across the cyber kill chain can help critical organisations to identify, prevent, stop, and prepare for any such cyber-attacks.

Continuous security validation across the cyber kill chain can help critical organisations to identify, prevent, stop, and prepare for any such cyber attacks.

References:

[1] https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks

[2] https://www.eccouncil.org/cyber-threat-intelligence/

[3] https://www.usprotech.com/7-essential-steps-cybersecurity-kill-chain-process/

CISA & NSA Release Guidance on Selecting and Hardening VPNs

Source: https://www.nsa.gov/

PRESS RELEASE | Sept. 28, 2021

NSA, CISA Release Guidance on Selecting and Hardening Remote Access VPNs

FORT MEADE, Md. – The National Security Agency and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint Cybersecurity Information Sheet today detailing factors to consider when choosing a virtual private network (VPN) and top configurations for deploying it securely. "Selecting and Hardening Remote Access VPN Solutions" also will help leaders in the Department of Defense, National Security Systems and the Defense Industrial Base better understand the risks associated with VPNs.

VPN servers are entry points into protected networks, making them attractive targets. Multiple nation-state advanced persistent threat (APT) actors have weaponized common vulnerabilities and exposures (CVEs) to gain access to vulnerable VPN devices. Exploitation of these CVEs can enable a malicious actor to steal credentials, remotely execute code, weaken encrypted traffic's

Virtual Private Networks (VPNs) allow users to connect to a corporate network remotely via a secure tunnel. Through this tunnel, off-site users can take advantage of the internal services and protections such as email/collaboration tools, sensitive document repositories, perimeter firewalls and gateways which normally make this entry point vulnerable to exploitation by threat actors. The United States National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) have released the cybersecurity information sheet that helps organisations select standards-based (rather than proprietary) VPN solutions and recommends hardening guidance to avoid compromise and respond to attacks. This joint CISA-NSA information sheet recommends to avoid selecting non-standard VPN solutions, including a class of products referred to as Secure Sockets Layer/Transport Layer Security (SSL/TLS) VPNs. This information sheet also describes how hardening the VPN against compromise can be achieved by reducing the VPN server's attack surface through Configuring strong, approved cryptographic protocols, algorithms, and authentication credentials, running only strictly essential features and Protecting access to and from the VPN. These recommendations are really essential for ensuring a network's cybersecurity.

This joint CISA-NSA information sheet recommends to avoid selecting non-standard VPN solutions, including a class of products referred to as Secure Sockets Layer/Transport Layer Security (SSL/TLS) VPNs.

Vulnerability Watch

Critical Vulnerability in Zoho ManageEngine ADSelfService

Source: https://us-cert.cisa.gov/, https://nvd.nist.gov/

ManageEngine
ServiceDesk Plus

Critical Improper Authentication vulnerability (CVE-2021-44077) has been discovered in Zoho ManageEngine ServiceDesk Plus. It has a CVSSv3 Base Score of 9.8. The flaw is related to /RestAPI URLs in a servlet, and ImportTechnicians in the Struts configuration. ServiceDesk Plus before 11306, ServiceDesk Plus MSP before 10530, and SupportCenter Plus before 11014 are affected by the flaw. Successful exploitation of the flaw may allow an attacker to upload executable files and place webshells, compromise administrator credentials, conduct lateral movement, and exfiltrate registry hives and Active Directory files. It is recommended to apply patches.

The flaw is related to /RestAPI URLs in a servlet, and ImportTechnicians in the Struts configuration.

Over 30,000 GitLab Servers Still Unpatched Against Critical Bug

Source: https://www.bleepingcomputer.com/, https://www.rapid7.com/

GitLab

Critical Unauthenticated Remote Code Execution vulnerability (CVE-2021-22205) which was patched more than six months ago is still being exploited in the wild. It has a CVSSv3 Base Score of 10.0. All versions of GitLab CE/EE starting from 11.9 are affected.

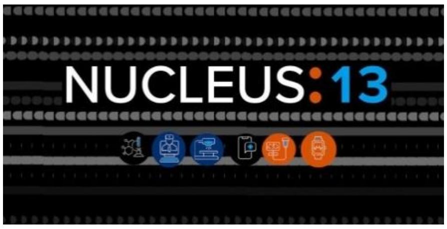
According to a report published by Rapid7, at least 50% of the 60,000 Internet-facing GitLab installations are not patched against the critical flaw. Admins need to update to 13.10.3, 13.9.6 or 13.8.8 versions to patch the flaw. In order to ensure that the GitLab instance isn't vulnerable to exploitation, one can check its response to POST requests that attempts to exploit ExifTool's mishandling of image files.

To ensure that the GitLab instance isn't vulnerable to exploitation, one can check its response to POST requests that attempts to exploit ExifTool's mishandling of image files.

13 TCP Security Bugs Impacts Critical Healthcare Devices

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

A total of 13 vulnerabilities dubbed as NUCLEUS: were discovered in the Nucleus Real-Time Operating System (RTOS) from Siemens that powers devices used in the aerospace, automotive, industrial and medical sectors. The set of flaws affects the Nucleus TCP/IP stack and could be leveraged to obtain remote code execution on vulnerable devices, create a denial-of-service condition, or obtain info that could lead to damaging consequences. Among the 13 vulnerabilities, CVE-2021-31886 is a critical bug affecting the FTP server component and remaining are of medium and high severity. Siemens has released updates to fix the vulnerabilities.



Vulnerability in GlobalProtect Portal and Gateway Interfaces

Source: https://security.paloaltonetworks.com/CVE-2021-3064

A critical memory corruption vulnerability was discovered in Palo Alto Networks GlobalProtect portal and gateway interfaces. It has a CVSSv3 Base Score of 9.8. The flaw enables an unauthenticated network-based attacker to disrupt system processes and potentially execute arbitrary code with root privileges. This issue affects only PAN-OS firewall configurations with a GlobalProtect portal or gateway enabled. This issue has been fixed in PAN-OS 8.1.17 and all later versions.

paloalto® NETWORKS

This issue affects only PAN-OS firewall configurations with a GlobalProtect portal or gateway enabled.

Critical Vulnerability in Cisco Products

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

Critical Remote Code Execution vulnerability (CVE-2021-34770) has been discovered in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Software for Cisco Catalyst 9000 Family Wireless Controllers. The OEM has given it a score of 10.0. The flaw is due to a logic error that occurs during the validation of CAPWAP packets. The flaw could allow an unauthenticated, remote attacker to execute arbitrary code with administrative privileges or cause a Denial of Service (DoS) condition on an affected device. Cisco has released software updates to address the flaw.

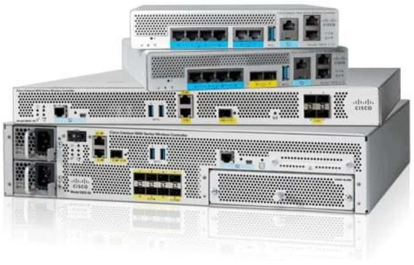


Image source: https://logging.apache.org/

Log4shell Vulnerability: Perspectives for Critical Sector Organisations

Kundapur Pradeep Bhat, NCIIPC

On 9th December 2021, a critical remote code execution vulnerability in the Java logging library log4j2 was publicly identified and tagged as CVE-2021-44228. The zero-day vulnerability, also called Log4shell, was discovered in the popular log4j2 open-source logging library maintained by Apache. The Log4j2 library is widely used and commonly embedded into a large number of Java software, including open-source software, cloud services and commercial applications The Log4shell vulnerability is rated 10 out of 10 on the CVSS due to the high severity of impact on an organisation in case it is leveraged by attackers.

Since the time of its public disclosure, the Log4shell vulnerability is being continuously monitored and researched by multiple security product vendors and independent cyber security professionals across the world, as well as by national cyber security organisations like CISA US, NCSC UK, CERT-In, NCIIPC et al. Many software applications and cloud services providers have been impacted but they have reacted swiftly and have mitigated the vulnerability to some extent.

The vulnerability is fairly simple to exploit, hence it is vital for all organisations, and especially those that perform critical functions, to quickly take action to protect their enterprise information infrastructure.

The vulnerability is fairly simple to exploit, hence it is vital for all organisations, and especially those that perform critical functions, to quickly take action to protect their enterprise information infrastructure. Organisations subscribing to threat intelligence feeds are being provided with regular updates on the detection, mitigation and remediation actions, as well as guidance to avoid the exploitation of this vulnerability. Recommendations are also available on predictive indicators that can be used to detect the current and potentially future attack variants.

Recommendations are also available on predictive indicators that can be used to detect the current and potentially future attack variants.

Given the organisational level impact of this vulnerability, National Cyber Security Centre, United Kingdom, in one of their blogs, has listed a set of questions that board members of medium to large organisations should be asking their IT teams. Organisations like Centre for Internet Security are also providing guidance to organisations on handling this vulnerability.

Almost all of the modern software is created using a ‘building blocks’ approach, in which the software development teams use well-known software libraries like Log4j2 and source code from public repositories rather than writing new code from scratch. For example, Github alone has over 470,132 projects depending on Log4j. Log4j2 is ubiquitous as an embedded software component in various devices, applications, services and supply chains. Many of these embedded versions are not obvious or documented. Hence, it is very likely that this vulnerability will be open to exploitation by attackers for a significantly long period.

US Presidential Executive Order 14028 dated 12 May 2021 has comprehensively described the term Software Bill of Materials (SBOM) as a nested inventory or list of components in a software product. The US National Telecommunications and Information Administration (NTIA) has further published the elements for an SBOM. The SBOM will emerge as a key building block in software security and software supply chain risk management. It will be useful to those who develop or manufacture software, those who select or purchase software, and those who operate software.

The SBOM will emerge as a key building block in software security and software supply chain risk management.

Organisations therefore will have to not only actively monitor, detect and mitigate the impact of this vulnerability in their current environments but should also have mechanisms such as SBOM in place that can be used to discover vulnerable components in their future procurements of software solutions and services, and in software that is deployed in production systems.

It will be useful to those who develop or manufacture software, those who select or purchase software, and those who operate software.

References:

[1] https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

[2] https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know

[3] https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIA D-2021-0046

[4] https://www.ncsc.gov.uk/blog-post/log4j-vulnerability-what-should-boards-be-asking

[5] https://www.cisecurity.org/log4j-zero-day-vulnerability-response/

[6] https://www.securonix.com/blog/securonix-security-advisory-detecting-apache-log4jlog4shell-cve-2021-44228-attacks-and-post-exploitation-activity

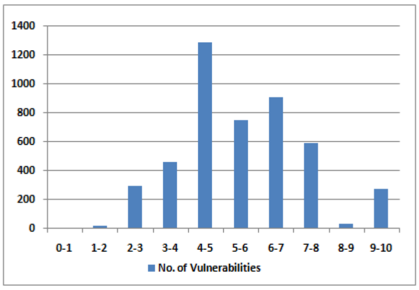
[7] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[8] https://ntia.gov/SBOM

Quarterly Vulnerability Analysis Report

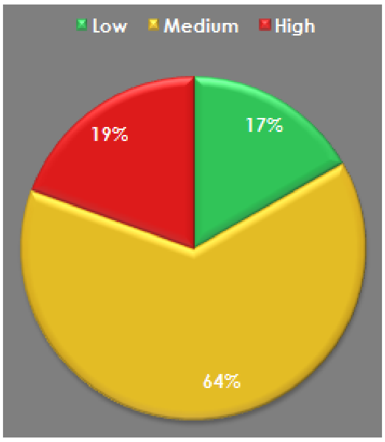
KMS Team, NCIIPC

A total of 4629 vulnerabilities have been observed during last quarter, out of which majority of vulnerabilities have score ranging from 4-7. 19 percent of total vulnerabilities reported were of high severity. Microsoft, Apple, Google, Adobe and Fedoraproject were the top five vendors having 30% of total reported vulnerabilities.



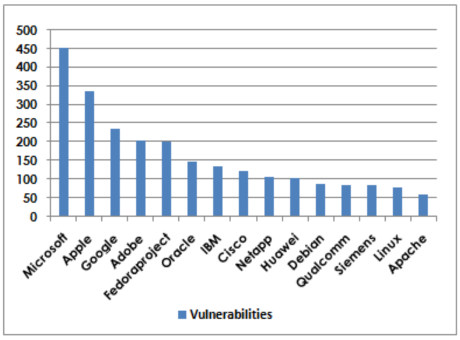
Severity-wise number of vulnerabilities

Severity	CVSS Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Sep	Oct	Nov		
Low	0-1	0	0	0	0	773
	1-2	4	9	7	20	
	2-3	71	106	117	294	
	3-4	164	164	131	459	
Medium	4-5	513	438	341	1292	2956
	5-6	219	310	223	752	
	6-7	396	258	258	912	
High	7-8	187	202	204	593	900
	8-9	10	13	9	32	
	9-10	139	58	78	275	
Total		1703	1558	1368		4629



Severity-wise share of vulnerabilities

S. No.	Vendor	No. of Vulnerabilities			Total
		Sep	Oct	Nov	
1.	Microsoft	197	105	152	454
2.	Apple	268	53	15	336
3.	Google	29	114	92	235
4.	Adobe	146	13	45	204
5.	Fedoraproject	53	99	49	201
6.	Oracle	6	138	3	147
7.	IBM	53	42	39	134
8.	Cisco	51	52	21	124
9.	Netapp	10	94	4	108
10.	Huawei	4	67	33	104
11.	Debian	45	35	9	89
12.	Qualcomm	35	31	18	84
13.	Siemens	40	24	20	84
14.	Linux	24	12	43	79
15.	Apache	20	17	24	61



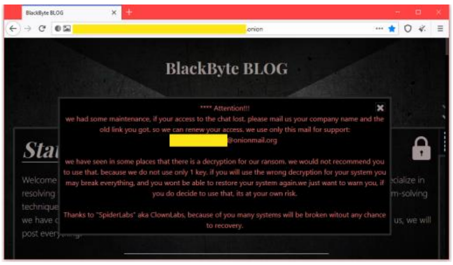
Count of vulnerabilities for top 15 vendors

Security App

BlackByte Ransomware Decryptor Released by TrustWave

Source: https://www.bleepingcomputer.com/, https://therecord.media/

A BlackByte ransomware decryptor has been released by TrustWave. This allows victims to recover their files and data for free. BlackByte ransomware written in C#, mainly targets corporate victims by terminating security mail server and databases to encrypt a device. It also disables Microsoft Defender on target devices before encryption. This ransomware downloads a file named 'forest.png', appears as image file it actually contains AES encryption key to encrypt device. In AES encryption same key is used for both encryption and decryption. Ransomware downloads encryption key and appends to the ransom note. During research it was found that same encryption key is used for multiple victims. Due to the same encryption key, Trustwave used this key to build a decryptor that recover victim's files. The source code of decryptor is available on github https://github.com/SpiderLabs/BlackByteDecryptor. To use it, user needs to download source code and compile. This decryptor will not work to recover data if different key is used for encryption.



**** Attention!!!
we had some maintenance, if your access to the chat lost. please mail us your company name and the old link you got. so we can renew your access. we use only this mail for support:
[redacted]@onionmail.org

we have seen in some places that there is a decryption for our ransom. we would not recommend you to use that. because we do not use only 1 key. if you will use the wrong decryption for your system you may break everything, and you wont be able to restore your system again.we just want to warn you, if you do decide to use that, its at your own risk.

Thanks to "SpiderLabs" aka ClownLabs, because of you many systems will be broken witout any chance to recovery.

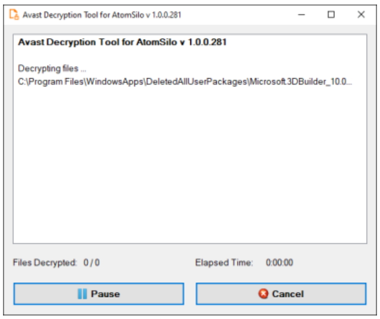
BlackByte gang warns companies about using the decrypter with the wrong key

BlackByte ransomware written in C#, mainly targets corporate victims by terminating security mail server and databases to encrypt a device.

Avast Released Decryptor for AtomSilo and LockFile Ransomware

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

Avast has released a decryption tool to decrypt files encrypted by AtomSilo and LockFile ransomware. Decryption tool can be downloaded from Avast's servers https://www.avast.com/en-in/ransomware-decryption-tools. LockFile ransomware exploits unpatched ProxyShell and PetitPotam vulnerabilities to encrypt devices. Ransomware appends .lockfile extension to the encrypted files' names and drop ransom notes named using the '[victim_name]-LOCKFILE-README.hta' format. Atom Silo ransomware operators have targeted Confluence Server and Data Center servers. Atom Silo uses side-loading malicious dynamic-link libraries to disrupt endpoint protection.



Avast Decryption Tool for AtomSilo v 1.0.0.281

Decrypting files ...
C:\Program Files\WindowsApps\DeletedAllUserPackages\Microsoft.3DBuilder_10.0...

Files Decrypted: 0 / 0 Elapsed Time: 0:00:00

Avast Decryption Tool for AtomSilo
Image source: https://decoded.avast.io/

Driftwood: Open Source Tool for Leaked Public-Private Key Pairs

Source: https://portswigger.net/

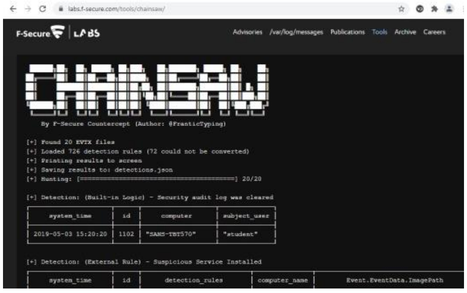
A new tool dubbed as Driftwood has come for discovery of leaked, paired private and public keys released in open-source community. It allows security professional to know if an identified encryption key is a sensitive key from online repositories. The tool uses Google's Certificate Transparency project, an open log of TLS certificates and GitHub SSH keys. Driftwood is able to take an asymmetric private key, extract the public key component and compare this key with TLS, SSH key database to check if it pairs

Driftwood is able to take an asymmetric private key, extract the public key component and compare this key with TLS, SSH key database to check if it pairs with sensitive key.

with sensitive key. This tool is available on GitHub and new key sources will be added in the future. This tool helps infosec professionals to find vulnerabilities so that they can revoke affected certificates as soon as possible.

Chainsaw Tool to Analyse Windows Event Logs

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



```
    By F-Secure Countercept (Author: @FranticTyping)

[+] Found 20 EVTX files
[+] Loaded 726 detection rules (72 could not be converted)
[+] Printing results to screen
[+] Saving results to: detections.json
[+] Hunting: [========================================] 20/20

[+] Detection: (Built-in Logic) - Security audit log was cleared

┌─────────────────────┬──────┬────────────────┬──────────────┐
│     system_time     │  id  │    computer    │ subject_user │
├─────────────────────┼──────┼────────────────┼──────────────┤
│ 2019-05-03 15:20:20 │ 1102 │ "SANS-TBT570"  │ "student"    │
└─────────────────────┴──────┴────────────────┴──────────────┘

[+] Detection: (External Rule) - Suspicious Service Installed

┌─────────────────────┬──────┬──────────────────┬───────────────┬─────────────────────────────
│     system_time     │  id  │ detection_rules  │ computer_name │   Event.EventData.ImagePath
```

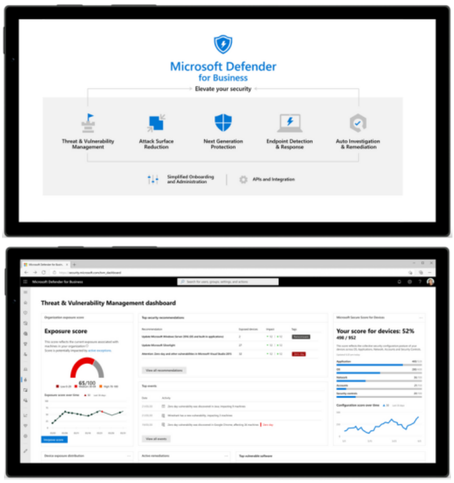
Image source: https://labs.f-secure.com/tools/chainsaw/

Chainsaw tool is a Rust-based command line utility to identify threats after analysing event logs. The tool is designed to help blue team in their investigation. It offers a generic and fast method of searching through event logs. It uses Sigma rule detection logic to find event logs related to the investigation. It uses EVTX parser library and F-Secure Countercept's TAU Engine library. This tool provides following features:

- It provides a simple interface to search through event logs by keyword, regex pattern or for specific event IDs.
- It can extract and parse Windows Defender, F-Secure, Sophos, and Kaspersky AV alerts.
- It detects users creation and addition to the sensitive group.
- Brute force of local user accounts.
- RDP logins, network logins etc.
- It provides result in ASCII table, CSV or JSON format.

Microsoft's New Endpoint Security Solution for SMBs

Source: techcommunity.microsoft.com, www.bleepingcomputer.com


Microsoft Defender
for Business
Elevate your security
Threat & Vulnerability Management
Attack Surface Reduction
Next Generation Protection
Endpoint Detection & Response
Auto Investigation & Remediation
Simplified Onboarding and Administration
APIs and Integration
Microsoft Defender for Business
Threat & Vulnerability Management dashboard
Exposure score
Your score for devices: 52%

Threat and Vulnerability management dashboard

A new endpoint security solution named as Microsoft Defender for Business, has been released by Microsoft for small and medium enterprises. It provides protection against cybersecurity threats, including malware and ransomware. It works on most of the available platforms such as Windows, macOS, ioS and Android devices. It provides simplified deployment and management for IT administrators. It has Threat and vulnerability management feature which alerts users for misconfiguration in software. It also has behavioural monitoring feature. It comes with simplified client configuration with wizard-driven setup and recommended security policies activated to make it easier to manage without dedicated security team.

SCADAfence Partners with Keysight Technologies

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

SCADAfence announced its partnership with Keysight Technologies. This partnership is aimed towards enhancing the cybersecurity of complex Operational Technology (OT) networks and boost their network visibility. This partnership brought together Keysight's network test access point (TAP) and network packet broker (NPB) solutions with SCADAfence's non-intrusive platform for deep packet inspection (DPI). The deployment of their solution together would increase real-time visibility into OT environments thereby providing detailed asset visibility and continuous threat detection for manufacturing sites, water and wastewater environments, automotive, oil and gas facilities and other industrial infrastructures.

Image source: scadafence.com, keysight.com

Siemens Launches AI Solution to Fight Industrial Cybercrime

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

Siemens Energy has launched a new cybersecurity solution platform, dubbed Eos.ii, for monitoring and responding to cyber threats against the Industrial Internet of Things (IIoT). This is an Artificial Intelligence (AI) and Machine Learning (ML) Security Information and Event Management (SIEM) platform that provides CISOs with a classic groundwork for industrial IoT cybersecurity. This SIEM platform collects and assembles data flows from IIoT endpoints for use by SOC teams, with insights brought together in one interface. The data flows from many endpoint devices are also standardised to reduce complex or junk data and give security teams a better chance of identifying anomalous behaviour. Additionally, Eos.ii automatically adapts defensive practices and prioritises high-impact events with the assistance of Machine Learning algorithms. As new threats emerge, Eos.ii seamlessly incorporates their known characteristics into automated defences and allows for easy manual updates to its rules-based detection engine. With Eos.ii, SOC teams spend less time on routine tasks and more time accompanying powerful investigations.

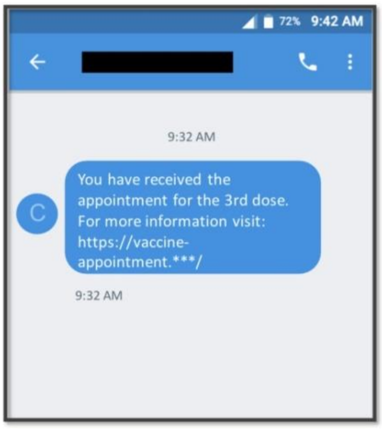
Image source: https://pbs.twimg.com/

This SIEM platform collects and assembles data flows from IIoT endpoints for use by SOC teams, with insights brought together in one interface.

Mobile Security

TangleBot targeting the United States and Canada

Source: https://www.cloudmark.com/en/blog/mobile/



[redacted]

9:32 AM

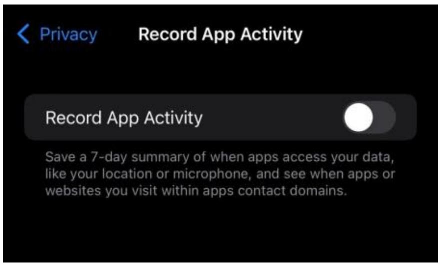
You have received the appointment for the 3rd dose. For more information visit: https://vaccine-appointment.***/

9:32 AM

A new SMS malware has been discovered targeting Android users in the United States and Canada. The malware lures its users by sending them text messages regarding COVID regulations. The SMS text messages contain a link to download the malware. Upon clicking on the link, the webpage notifies that the device's Adobe Flash Player is out of date and must be updated, which leads to the installation of malware in user's device. TangleBot then asks for permissions such as Accessibility services, contacts, SMS, call logs, Internet, camera, microphone and GPS etc. It then creates an overlay over financial apps installed in the victim's device to steal account credentials. It can also be used to exfiltrate victim's personal information and can spy on its victim.

Apple's Record App Activity

Source: https://www.zdnet.com/article/, https://developer.apple.com/



Record App Activity

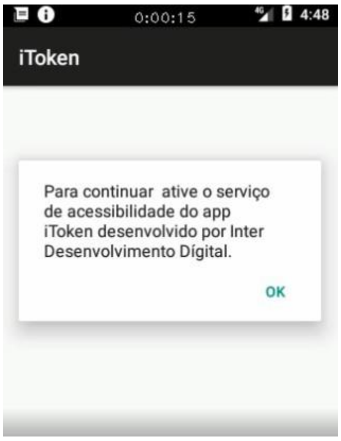
Record App Activity ○

Save a 7-day summary of when apps access your data, like your location or microphone, and see when apps or websites you visit within apps contact domains.

Starting from iOS 15.2, iPadOS 15.2, and watchOS 8.3 or later, Apple has added a new feature called 'Record App Activity' in its privacy settings. If turned on, it generates analytics of installed apps for the last seven days. The analytics contain record of the resources that the app has accessed. Resources may be defined as the device's camera, user's contacts, location data, user's media library, device's microphone, user's photo library and screen sharing. The analytics also contained timestamp of when the resources were accessed. This will help to identify whether an app is behaving suspiciously.

PixStealer attacking Brazilian Bank

Source: https://research.checkpoint.com/2021/



iToken

Para continuar ative o serviço de acessibilidade do app iToken desenvolvido por Inter Desenvolvimento Digital.

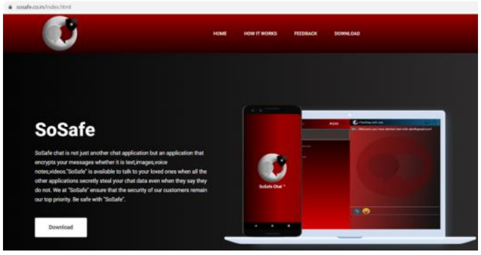
OK

During the COVID-19 pandemic, instant payments solution created by the Central bank of Brazil, Pix, is being targeted by malicious actors. Check Point Research has discovered PixStealer malware ("Pag Cashback 1.4") targeting the PagBank in Brazil. Its main function is to steal victim's money by abusing Android's Accessibility Service with no communication from C&C server. PixStealer's "big brother", MalRhino, is found to be more robust in nature as it can communicate with C&C server. It poses as fake iToken app for Brazilian Inter Bank. It uses JavaScript via Mozilla's Rhino Framework and abuses an open-source rhino-android library to perform its operations by remote code execution. To safeguard themselves, users are requested to download genuine apps from official Google Play Store only.

SoSafe Chat Application Targeting Indian Armed Forces

Source: https://blog.cyble.com/2021/11/11/

Cyble Research Labs have discovered an android Gravity RAT malware named SoSafe Chat which poses as a genuine chatting application. It was hosted on sosafe[.]co[.]in and believed to be targeting Indian Armed Forces. Its icon is similar to messaging app icons and requests for forty-two different permissions. An attacker can abuse thirteen of these permissions to exfiltrate SMS data, contacts data, current network information, device's location, files from device's external storage and send it to its C&C server. Users are requested to keep their anti-virus software in mobile devices up to date for detection and removal of these malware applications. It is also advised to download and install applications from official Play Store only.



sosafe.co.in/index.html

SoSafe

SoSafe chat is not just another chat application but an application that encrypts your messages whether it is text,images,voice notes,videos."SoSafe" is available to talk to your loved ones when all the other applications secretly steal your chat data even when they say they do not. We at "SoSafe" ensure that the security of our customers remain our top priority. Be safe with "SoSafe".

Rooting Malware Hits Popular App Play Stores

Source: https://resources.lookout.com/blog/

Researchers at the Lookout Threat Lab have discovered "AbstractEmu", a rooting malware, being distributed via Google Play Store, Amazon Appstore and Samsung Galaxy Store etc. with more than 10,000 downloads. AbstractEmu disguises itself as utility app, password manager, system tool etc. It leverages on vulnerabilities such as CVE-2020-0041, CVE-2020-0069 and CVE-2019-2215 to exploit android devices by gaining privileged access during rooting process. After installation, the malware uses code abstraction and anti-emulation techniques to avoid detection. The malware contains hidden files which includes shell codes and encoded binaries from popular rooting app 'Magisk' to ensure smooth rooting process. After rooting, it disguises itself as "Settings Storage" app in android device. The malware communicates with its C2 server via HTTP and in return, it receives JSON commands to execute. The malware is able to access contacts, call logs, SMS messages, location, camera and microphone etc. Out of the 17 victimised countries, United States is the most impacted one.

https://www.similarplay.com › ... › Lite Launcher ▾

Lite Launcher - Smart & Fast Launcherfor Android - APK ...

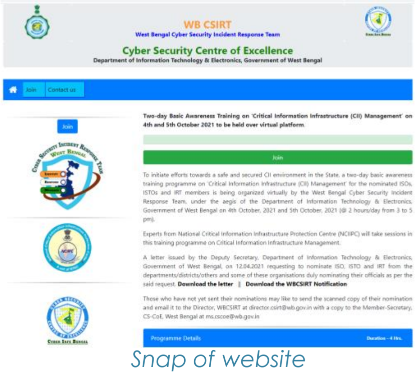
Top Dev : · Pegi : PEGI 3 · Publish Date : Feb 20, 2020 · Update Date : January 19, 2021 · File Size : 6.4M · Version : 1.8 · Installs : 10,000+ · Op. System : 4.3 and ...

It leverages on vulnerabilities such as CVE-2020-0041, CVE-2020-0069 and CVE-2019-2215 to exploit android devices by gaining privileged access during rooting process.

NCIIPC Initiatives

Cyber Security Awareness Program with Govt. of West Bengal

Program inauguration by Sh. H. K. Kusumakar (IPS), CISO - Govt of West Bengal



WB CSIRT
West Bengal Cyber Security Incident Response Team
Cyber Security Centre of Excellence
Department of Information Technology & Electronics, Government of West Bengal

Two-day Basic Awareness Training on 'Critical Information Infrastructure (CII) Management' on 4th and 5th October 2021 to be held over virtual platform.

To initiate efforts towards a safe and secured CII environment in the State, a two-day basic awareness training programme on 'Critical Information Infrastructure (CII) Management' for the nominated ISOs, ISTOs and IRT members is being organized virtually by the West Bengal Cyber Security Incident Response Team, under the aegis of the Department of Information Technology & Electronics, Government of West Bengal on 4th October, 2021 and 5th October, 2021 (@ 2 hours/day from 3 to 5 pm).

Experts from National Critical Information Infrastructure Protection Centre (NCIIPC) will take sessions in this training programme on Critical Information Infrastructure Management.

A letter issued by the Deputy Secretary, Department of Information Technology & Electronics, Government of West Bengal, on 12.04.2021 requesting to nominate ISO, ISTO and IRT from the departments/districts/others and some of these organisations duly nominating their officials as per the said request. **Download the letter | Download the WBCSIRT Notification**

Those who have not yet sent their nominations may like to send the scanned copy of their nomination and email it to the Director, WBCSIRT at director.csirt@wb.gov.in with a copy to the Member-Secretary, CS-CoE, West Bengal at ms.cscoe@wb.gov.in

Programme Details Duration - 4 Hrs.

Snap of website

Live interactive session for State's Critical Information Infrastructure (CII) Managers
National Cyber Security Awareness Month (NCSAM) October, 2021
Best Practices
Critical Information Infrastructure Protection
Risk Management
Data Integrity
Strategic Planning
Cyber Security
Auditing Methodology
Research & Development
Vulnerability Assessment
PSU
Cyber Safe Bengal

Inaugural session by Joint Secretary, IT&E Dept

NCIIPC conducted a two-day basic Awareness training on 'Critical Information Infrastructure (CII) Management' on 4th and 5th October 2021 on virtual platform. Approximately 150+ government officials, managing the CIIs of Government of West Bengal, joined this session. The program was inaugurated by Sh. H.K. Kusumakar (IPS), Chief Information Security Officer (CISO) - Government of West Bengal. Dr. Piyush Sharma, Director East Zone delivered the key note during opening session. The deliberation started with setting of learning objectives and applicability w.r.t the CII protection and its importance, by Sh. Tathagata Datta of NCIIPC. In the first session held on 04 Oct 2021 the training was imparted on 'Cyber Attack'. Major focus was given on various threat actors, including Malwares, their mode of propagation and most importantly the methods of their containment. During second session, on 05 Oct 2021 the training was imparted on 'Cyber Defence'. Security by Design framework, importance of Network Traffic Analysis and workings of Security Operations Centre were discussed.

Another program on 7th October was inaugurated by Joint Secretary, Information Technology and Electronics (IT&E), Government of West Bengal. Notable participation was from different government departments including State Data Centre, State WAN, Power Utilities, State Police and private sector entities. The session was fully interactive and NCIIPC representatives responded to the queries on various challenges faced by the critical sector organisations. The importance of identification of CII and their protection was elaborated to the participants. At the end of session, a quiz was conducted and both NCIIPC and Government of West Bengal jointly felicitated the winners.

NCIIPC raised concerns about the cyber threats and explained the necessity of cyber security awareness for smooth functioning of BFSI and Telecom Sector organisations.

Webinar on Cyber Security Awareness for BFSI & Telecom Sector

A webinar was organised for BFSI & Telecom sectors by NCIIPC on 29th October 2021. There were more than 90 participants from various banks, ministries and telecom sector organisations across the country, who participated in online webinar program. NCIIPC raised concerns about emerging cyber threats and explained the necessity of cyber security awareness for smooth functioning of BFSI and Telecom Sector organisations. Sh. Mathan Babu K, CISO, Vodafone Idea (VI) Ltd. delivered presentation on 'Convergence of Industries & Its significance to Cyber Security'. Sh. Tathagatta Datta, Consultant, NCIIPC delivered lecture on 'Importance of Regulatory Cyber Security Controls'. Sh. Sanjay Katkar, Joint MD & CTO, Quick Heal Technologies presented on 'Telecom & BFSI Threat Landscape'. Sh. Sriniwasa Bhoosarapu from PFRDA informed that PFRDA and IRDA also released their cyber security guidelines. Thereafter, Sh. T R Venkateswaran, CISO, PNB delivered his presentation on ‘Digital Payment Security Controls’. The webinar was concluded with vote of thanks by Director NCIIPC (West).

Webinar on Importance of Cyber Security for CII

Director, NCIIPC (South) delivered presentation at a webinar on Importance of Cyber Security for Critical Information Infrastructure, for National Hydroelectric Power Corporation (NHPC) on 13 October 2021. It was attended by the participants from NHPC units/centres across the country. Following topics were covered during the presentation:

- NCIIPC & its mandate
- Critical Sectors & Critical Information Infrastructure (CII)
- Major Functions of NCIIPC
- What is Critical in Power Sector
- Necessity of Cyber Security in Power Sector
- Govt. of India Initiatives in Power Sector
- Areas to Focus
- Steps required to be undertaken at National Level
- Steps required to be undertaken at Organisational Level
- What other nations are doing to protect their CII
- Threat & Vulnerability Statistics

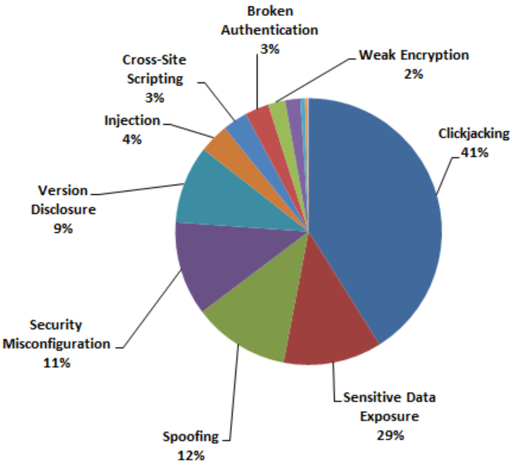
Director, NCIIPC (South) delivered presentation at a webinar on Importance of Cyber Security for Critical Information Infrastructure, for National Hydroelectric Power Corporation (NHPC) on 13 October 2021.

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 2265 vulnerabilities reported during the last quarter of 2021. The top 10 vulnerabilities are:

- Click Jacking
- Sensitive Data Exposure
- Spoofing
- Security Misconfiguration
- Version Disclosure
- Injection
- Cross-Site Scripting
- Broken Authentication
- Weak Encryption
- Application Logic



Around 307 researchers participated in RVDP programme during the last quarter of 2021. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Ashish Khare
- Banavath Aravind
- CyberPeace Foundation
- Jay Kumar Pandey
- Joshua Arulsamy
- M Sathvika Sai
- Manab Jyoti Dowarah
- Navdeep Singh
- Naved Shaikh
- Prince Prafull
- Rushabh Vyas
- Sarathlal Srl
- Shubhdeep
- Tushar
- Vishnu Vardhan

NPTI Conducted Seminar on Cyber Security Increasing Cyber Resilience of the Nation

Sh. Alok Kumar, Secretary (Power), addressing the seminar

A One-Day National Seminar on Cyber Security 'Increasing Cyber Resilience of the Nation' was organised by National Power Training Institute (NPTI) along with Central Electricity Authority (CEA) on 28 October 2021. Sh. Alok Kumar, Secretary (Power), Ministry of Power, Govt. of India & Chairman Governing Council, NPTI, was the chief guest of the seminar. The seminar was organised with objective of securing the Critical Information Infrastructure of Power Sector Utilities. Faculty for this seminar were industry experts and officials from CEA and NCIIPC Sh. Pradeep Bhat, Consultant, NCIIPC was one of the panel members. The seminar covered the following topics:

- Importance of Cyber Security in Indian Power Sector.
- Establishing Baseline Measure for Cyber Security.
- Capacity building through Education & Training on Security of Cyber Physical Systems.
- Panel Discussion on 'Role of On-The-Job Training in Cyber Security'

NCIIPC Supports Global CyberPeace Challenge

The CyberPeace Foundation jointly with Autobot Infosec has organised Global CyberPeace Challenge 3.0 supported by Ministry of Electronics and Information Technology (MeitY), Cybersecurity Center of Excellence (DSCI-Government of Telangana), Office of the Principal Scientific Advisor and NCIIPC along with others for promoting Cyber Safe Nation. More than 70 countries have participated in this cyber challenge. Global CyberPeace Challenge 3 has been organised with three challenges: Cyber Policy & Strategy Challenge, Peace-a-Thon: The innovation challenge and Capture the Flag (CTF).

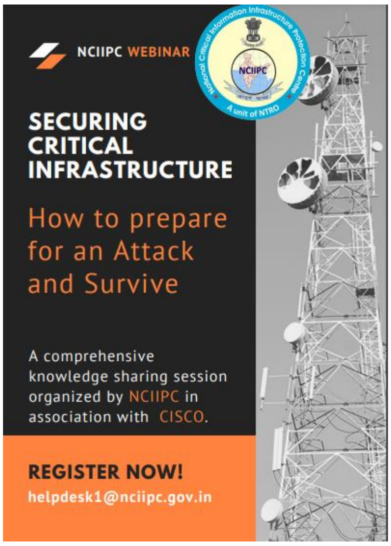
NCIIPC and CISCO Webinar on Securing Critical Infrastructure

A one day webinar on 'Securing Critical Infrastructure - How to prepare for an Attack and Survive' was organised by NCIIPC in association with CISCO on 23 November 2021. Participants were from various ministries, banks and other organisations across the country. First session of the webinar was presented by Sh. KMP Das and Sh. Simon Finn, Security and Trust Office. They talked on 'Securing Critical Infrastructure' that covered:

- Principles and challenges for securing critical infrastructure
- State of Cybersecurity in India
- Challenges in dealing with critical infrastructure
- IT/OT interdependence: Silos
- Evolving cyber maturity to lower risk
- Protect the unprotected

The second session was presented by Sh. Ashraf Ali, Leader - Systems Engineering, Cyber Security Business, Cisco - India. He delivered presentation on 'Cyber Attack methods & How to build your defence against them' that covered:

- Past Cyber Attacks & Most common methods
- Architectural approach for Effective Defence



NCIIPC WEBINAR

SECURING CRITICAL INFRASTRUCTURE

How to prepare for an Attack and Survive

A comprehensive knowledge sharing session organized by NCIIPC in association with CISCO.

REGISTER NOW!
helpdesk1@nciipc.gov.in

Upcoming Events - Global

January 2022

World Conference on Cyber Security and Ethical Hacking, Singapore	2-3 Jan
Real World Crypto Symposium, Amsterdam	10-12 Jan
Ascent: Spotlight on Cybersecurity, Virtual	12 Jan
International Conference on Mobile Application Security, Bali	14-15 Jan
6th International Conference on Cryptography, Security and Privacy, Tianjin	14-16 Jan
15th International Conference on Computers, Privacy and Data Protection, Brussels	26-28 Jan
23rd PCI London, London	26 Jan
Sum of all fears – Nordic IT Security, Stockholm	27 Jan

February 2022

Fundamentals of CDO Leadership in Data-Driven Enterprises, Miami	3-4 Feb
CactusCon 10 (2022), Mesa	4-5 Feb
5G EXPO 2022, Florida	8-11Feb
International Conference on Information Systems Security and Privacy 2022, Virtual	9-10 Feb
Algorithm Conference 2022, Dallas	10-12 Feb
AppSec New Zealand 2022, Auckland	17-18 Feb
Blockchain in Healthcare Symposium 2022, Dubai	22-23 Feb
CyberSecAsia Virtual Summit 2022, Virtual	23-24 Feb

March 2022

Cyber Intelligence Europe 2022, Oslo	1-3 Mar
Cloud & Cyber Security Expo, London	2-3 Mar
IEEE 7th International Conference on Big Data Analytics, Guangzhou	4-6 Mar
Cyber Security for Manufacturing Summit Europe, Munich	8-9 Mar
11th International Conference on Frontiers of Information Technology, Paris	14-16 Mar
17th International Conference on Cyber Warfare and Security, New York City	17-18 Mar
BSides Dublin 2022, Dublin	19 Mar
Cyber Security for Critical Assets USA Summit 2022, Texas	29-30 Mar

JANUARY 12TH, 2022

Ascent: Spotlight on Cybersecurity

Nordic IT Security
knowledge is the best defence

JANUARY 2022

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

FEBRUARY 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					

BLOCKCHAIN IN HEALTHCARE

International Conference on Frontiers of Information Technology
11th
ICFIT 2022
PARIS, FRANCE
MARCH 14-16, 2022

April 2022

7th Annual Big Data and Analytics, Toronto	5-6 Apr
5th International Conference on Information Science and Systems, Beijing	15-17 Apr
AI in RegTech Summit 2022, New York	21-22 Apr
7th International Conference on Internet of Things, Big Data and Security, Virtual	22-24 Apr
Big Data Technology Warsaw Summit 2022, Virtual	26-28 Apr
Cyber Security for Critical Assets Asia 2022, Singapore	26-27 Apr
11th Computer Science On-line Conference 2022, Virtual	26-30 Apr
BSides Charm 2022, Baltimore	30 Apr

MARCH 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		

Upcoming Events - India

International Conference on Communication Systems & Networks, Bengaluru	3-9 Jan
Convergence India 2022, New Delhi	23-25 Mar
Internet of Things India Expo 2022, New Delhi	23-25 Mar
Global Digital Security Forum India 2022, Mumbai	19-20 May

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

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

- AI: Artificial Intelligence
- APT: Advanced Persistent Threat
- C&C: Command and Control
- CAPWAP: Control and Provisioning of Wireless Access Point
- CDSL: Central Depository Services Limited
- CEA: Central Electricity Authority
- CERT: Computer Emergency Response Team
- CII: Critical Information Infrastructure
- CIRT: Computer Incident and Response Team
- CISA: Cybersecurity and Infrastructure Security Agency
- CISO: Chief Information Security Officer
- CSIRT: Computer Security Incident Response Team
- CSOC: Cyber Security Operation Centre
- CTF: Capture the Flag
- CTI: Cyber Threat Intelligence
- CVE: Common Vulnerabilities Exposure
- CVL: CDSL Ventures Limited
- CVSS: Common Vulnerability Scoring System
- DOS: Denial of Service
- DoT: Department of Telecommunications
- DPI: Deep Packet Inspection
- HIPS: Host-based Intrusion Prevention System
- I-CAMPS: Indian Citizens Assistance for Mobile Privacy & Security
- IIOT: Industrial Internet of Things
- IoC: Indicators of compromise
- IR: Incident Response
- IRDA: Insurance Regulatory and Development Authority
- IT&E: Information Technology and Electronics
- ITU: International Telecommunication Union
- LDAP: Lightweight Directory Access Protocol
- MeitY: Ministry of Electronics and Information Technology
- MISP: Malware Information Sharing Platform
- ML: Machine Learning
- NCSAM: National Cyber Security Awareness Month
- NIC: National Informatics Centre
- NPB: Network Packet Broker
- NPTI: National Power Training Institute
- NSA: National Security Agency
- NSCS: National Security Council Secretariat
- NTIA: National Telecommunications and Information Administration
- OCAC: Odisha Computer Application Centre
- PFRDA: Pension Fund Regulatory and Development Authority
- RAT: Remote Access Trojan

- RCE: Remote Code Execution
- RTOS: Real-Time Operating System
- RTT: Round-Trip Time
- SBOM: Software Bill of Materials
- SIEM: Security Information and Event Management
- SMB: Server Message Block
- SOC: Security Operations Centre
- SSID: Service Set Identifier
- TAP: Test Access Point
- TTP: Tools, Techniques and Procedures
- UN: United Nations
- VPN: Virtual Private Network

Notes

Feedback/Contribution

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

Disclaimer

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