NEWSLETTER

January 2023

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

14th January

NCIIPC Foundation Day

e-Gov
National Critical Information Infrastructure Protection Centre
NCIIPC
A unit of NTRO

Government

Health

Banking, Finance & Insurance

Telecom

Power & Energy

Transport

Strategic & Public Enterprises

Jun 2013 *Guidelines for Protection of National CII Released*

Jan 2014 *Formation of NCIIPC*

Jan 2015 *Guidelines for Protection of National CII Version 2.0 Released*

Dec 2015 *UIDAI-CIDR Notified as "Protected System"*

Feb 2016 *LRIT System, Directorate General of Shipping Declared as "Protected System"*

Jan 2017 *First Edition of NCIIPC Newsletter Released*

Aug 2017 *NCIIPC extended its presence on Social Media Platforms*

May 2018 *Rules of "Information Security Practices and Procedures for Protected System" Notified*

Jan 2023 *50+ CII Declared as "Protected System" till date*

https://nciipc.gov.in/

@NCIIPC

NCIIPC India

NCIIPC India

helpdesk1@nciipc.gov.in

1800-11-4430

VOLUME 7 ISSUE 1

@NCIIPC

NCIIPC Newsletter

January 2023

स्वच्छ भारत

एक कदम स्वच्छता की ओर

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

In January 2023, NCIIPC completed 9 years of its inception. It was 14th January 2014 when NCIIPC was raised through a Gazette notification. Since then NCIIPC has gone a long way for identification and protection of National Critical Information Infrastructure (CII).

In last few years there has been a great leap in cyber security incidents including ransomware attacks observed across the globe. India has also encountered similar attacks on its CII. Cyber criminals are mostly using social engineering tactics to enter into the enterprise networks. Once successful, they scan and exploit the prominent vulnerabilities to gain access and propagate laterally into the other network systems. System/Network compromise happens through exploitation of known vulnerabilities to execute malicious binaries, exploiting remote access protocols and devices, credential theft, availing tools already existing within target environment to evade detection etc. Once compromised, the system files are encrypted and ransom is sought for retrieval of the critical data. Cyber criminals sometimes also threaten to disclose private information in the public/darkweb forums. Sensitising the employees regarding Social Engineering attacks is a must. Regular offline backup of the data will help organisations to restore fast in case of ransomware attack. Apart from this, organisatons should monitor the system and network logs for detection of suspicious activities. Strong password policy along with Multi Factor Authentication should be followed and systems should be updated on regular basis.

As part of capacity building activities, NCIIPC engaged with Critical Sector Organisations by organising a number of cyber security awareness activities during last year cyber security awareness month (Oct 2022). Large number of employees from Critical Sector Organisations participated in number of awareness webinars and Quiz.

Please do provide your suggestions / feedback to us on newsletter@nciipc.gov.in

News Snippets - National

India-Australia Fifth Cyber Policy Dialogue

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

On 17 November 2022, India and Australia held their fifth Bilateral Cyber Policy Dialogue in New Delhi. The Cyber Policy Dialogue was held with assistance of the India-Australia Framework Arrangement on Cyber and Cyber-Enabled Critical Technology Cooperation and Plan of Action 2020-2025 for a comprehensive and deeper cyber cooperation. The Indian delegation consisted of senior officials from National Security Council Secretariat (NSCS), Ministry of Electronics and Information technology (MEITY), Ministry of Home Affairs (MHA), Department of Telecommunications (DoT), National Critical Information Infrastructure Protection Centre (NCIIPC), and CERT-In. The Australian delegation comprised of senior officials from the Department of Home Affairs, Department of Foreign Affairs and Trade, Department of Industry Science and Resources, and the Australian Federal Police. Both sides agreed to explore opportunities for further collaboration with the private sector and academia, through the Australia-India Cyber and Critical Technology Partnership. Moreover, Australia and India are to jointly conduct Cyber Bootcamp, along with Cyber and Tech Policy Exchanges in collaboration with Indo-Pacific partners.

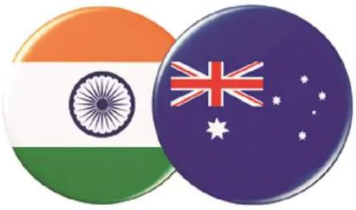


Image source: https://bsmedia.business-standard.com/

Both sides agreed to explore opportunities for further collaboration with the private sector and academia, including through the Australia-India Cyber and Critical Technology Partnership.

Release of Draft Data Protection Regulation

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

The Indian government released draft version of the data protection regulation 'The Digital Personal Data Protection Bill 2022' on 18 November 2022. The Bill aims to establish a comprehensive legal framework governing the digital personal data protection in India. The Bill allows the processing of digital personal data in a manner that recognises the right of individuals to protect their personal data, societal rights and the need to process personal data for lawful purposes. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules provide the security practices and procedures that a body corporate or any person collecting, possessing, storing, receiving, or handling information on behalf of the body corporate is required to observe for protecting personal data of users. These practices and procedures include the requirements that such body corporate or person need to publish on the website like:

- A policy for privacy and disclosure of data or information,
- To use information collected for the purpose for which it has been collected,

The Bill allows the processing of digital personal data in a manner that recognises the right of individuals to protect their personal data, societal rights and the need to process personal data for lawful purposes.

- To keep it secure and to obtain prior permission of the information provider for disclosing personal data.

Electricity Grid of India Soon to be Insulated from Cyber Attacks

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

Union Power Minister Sh. RK Singh has said that India's power network soon would be more future-ready and insulated from cyber-attacks with the provision of routine inspections and timely action under the Electricity Amendment Bill. The power ministry has made a provision for inspecting the national electricity grid in order to maintain cyber hygiene in the network through the Electricity Amendment Bill 2022. The bill provides for amending section 26 of the Act so as to strengthen the functioning of the National Load Despatch Centre (NLDC) for ensuring the grid's safety and security and for the economic and efficient operation of the nation's power system.

The power ministry has made a provision for inspecting the national electricity grid in order to maintain cyber hygiene in the network through the Electricity Amendment Bill 2022.

Cyber Attack on Central Depository Services (India) Limited

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

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

Central Depository Services (India) Limited (CDSL) discovered a cyber-attack on a few of its internal machines on 18 November 2022. The trade-related activity and back-end operations at brokerages were disrupted due to this malware attack. The company immediately isolated the infected machines and disconnected itself from other constituents of the capital market. The CDSL team reported the incident to the relevant authorities and worked with its cyber security advisors to analyse the impact. CDSL declared that the confidential information or investor data were not compromised. On 20 November 2022, the CDSL systems were made live after due checks and validations, within 48 hours of attack.

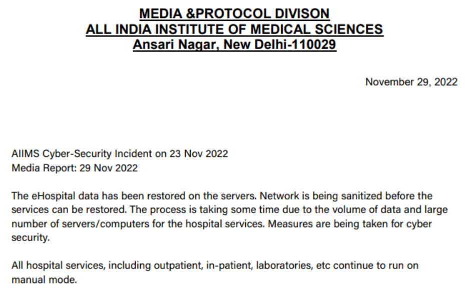
CDSL declared that the confidential information or investor data were not compromised.

Cyber Attack on AIIMS New Delhi

Source: hindustantimes.com, indiatoday.in, business-standard.com

Image source: https://aiims.edu/

All India Institute of Medical Sciences (AIIMS) New Delhi was hit by ransomware on 23rd November 2022. The staff was unable to access the mainstay hospital management application called eHospital. The patient care services in emergency, inpatient, outpatient and laboratory wings were managed manually after the server went down. Experts from India's Computer Emergency Response Team (Cert-In) examined the affected servers and on 24 November found that four servers (two application servers, one database server and one back-up server), were infected leading to multiple databases being encrypted. All infected servers were disconnected by the National Informatics Centre (NIC) team, which manages the eHospital system, to avoid further contamination of other servers. It was found that the firewall deployed to protect the AIIMS network was not properly configured. After more than two weeks the data was retrieved from an unaffected backup server and most of hospital services were restored. The Indian Computer Emergency Response Team, Delhi cybercrime special cell, Indian Cybercrime Coordination Centre, Intelligence Bureau, Central Bureau of Investigation (CBI), National Forensic Sciences University, National Critical Information Infrastructure Protection Centre and NIA, among others, were part of the investigation team.



MEDIA &PROTOCOL DIVISON
ALL INDIA INSTITUTE OF MEDICAL SCIENCES
Ansari Nagar, New Delhi-110029

November 29, 2022

AIIMS Cyber-Security Incident on 23 Nov 2022
Media Report: 29 Nov 2022

The eHospital data has been restored on the servers. Network is being sanitized before the services can be restored. The process is taking some time due to the volume of data and large number of servers/computers for the hospital services. Measures are being taken for cyber security.

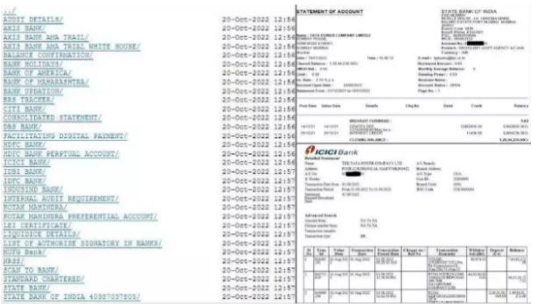
All hospital services, including outpatient, in-patient, laboratories, etc continue to run on manual mode.

Image source: https://twitter.com/

Tata Power Company Hit by Cyberattack

Source: https://archives.nseindia.com, www.hindustantimes.com

On 14 October 2022, Tata Power disclosed that its Information Technology infrastructure was hit by a cyberattack and some of its systems were affected as a result of it. Tata Power Company took steps to retrieve and restore the affected systems. All critical operational systems were restored. Restrictive access and preventive checks were put in place for employees and customer facing portals and touch points. Hive threat group claimed responsibility for the cyberattack and released the hacked data on their dark web forum. The leaked data included bank accounts of the company, details and bank statements of its employees including their remuneration and passport information. The leaked data also included details of the batteries used by Tata Power and diagrams of some of their grids.



```
../
AUDIT DETAILS/                                    20-Oct-2022 12:56
AXIS BANK/                                        20-Oct-2022 12:56
AXIS BANK ANA TRAIL/                              20-Oct-2022 12:56
AXIS BANK ANA TRIAL WHITE HOUSE/                  20-Oct-2022 12:56
BALANCE CONFIRMATION/                             20-Oct-2022 12:56
BANK HOLIDAYS/                                    20-Oct-2022 12:56
BANK OF AMERICA/                                  20-Oct-2022 12:56
BANK OF MAHARASHTRA/                              20-Oct-2022 12:56
BANK UPDATION/                                    20-Oct-2022 12:56
BRS TRACKER/                                      20-Oct-2022 12:56
CITI BANK/                                        20-Oct-2022 12:56
CONSOLIDATED STATEMENT/                           20-Oct-2022 12:56
DBS BANK/                                         20-Oct-2022 12:56
FACILITATING DIGITAL PAYMENT/                     20-Oct-2022 12:56
HDFC BANK/                                        20-Oct-2022 12:56
HDFC BANK PERPTUAL ACCOUNT/                       20-Oct-2022 12:56
ICICI BANK/                                       20-Oct-2022 12:56
IDBI BANK/                                        20-Oct-2022 12:57
IDFC BANK/                                        20-Oct-2022 12:57
INDUSIND BANK/                                    20-Oct-2022 12:57
INTERNAL AUDIT REQUIREMENT/                       20-Oct-2022 12:57
KOTAK MAHINDRA/                                   20-Oct-2022 12:57
KOTAK MAHINDRA PREFERENTIAL ACCOUNT/              20-Oct-2022 12:57
LEI CERTIFICATE/                                  20-Oct-2022 12:57
LIQUIDICE DETAILS/                                20-Oct-2022 12:57
LIST OF AUTHORISE SIGNATORY IN BANKS/             20-Oct-2022 12:57
MUFG Bank/                                        20-Oct-2022 12:57
NBSS/                                             20-Oct-2022 12:57
SCAN TO BANK/                                     20-Oct-2022 12:57
STANDARD CHARTERED/                               20-Oct-2022 12:57
STATE BANK/                                       20-Oct-2022 12:57
STATE BANK OF INDIA 40387037805/                  20-Oct-2022 12:57
```

Tata Power banking records (Source: Twitter post by Rakesh Krishnan)

News Snippets - International

The European Parliament's Website Attacked

Source: https://www.europarl.europa.eu/, https://www.euronews.com/

Image source: www.europarl.europa.eu/

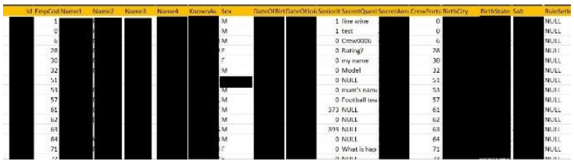
A sophisticated cyberattack targeted the European Parliament website on 23 November 2022, just after members voted to declare Russia a state sponsor of terrorism over its alleged attacks on Ukraine. The European parliament website was targeted by a Distributed Denial of Service (DDoS) attack designed to force high levels of outside traffic onto the site's server, disrupting the network. The Multimedia Centre for the Parliament, which runs as a separate website, remained unaffected.

AirAsia's Network Attacked by Daixin Threat Actors

Source: https://www.databreaches.net/, https://techmonitor.ai/

Image source: www.airasia.co.in/

Malaysia's largest airline company AirAsia suffered a massive ransomware attack on 11 and 12 November that compromised the sensitive personal information of millions of customers and employees. The stolen information included date of birth, country of birth, where that person is from, when employed for employees and the secret question and answer used to secure accounts. The threat actors obtained the personal data of 5 million unique passengers and all employees. Daixin threat actors encrypted a lot of resources and deleted backups. The threat actors avoided locking XEN, RHEL – hosts of flying equipment (radars, air traffic control, etc.), they avoided encrypting or destroying anything if the result could be life-threatening. The Daixin group's spokesperson stated that AirAsia's IT infrastructure was chaotic, poorly-secured and the internal network was configured without any rules.

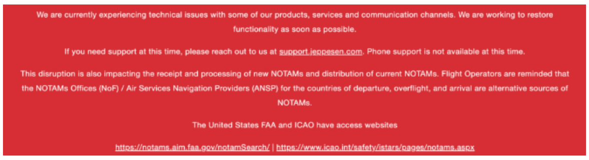


Id	EmpCod	Name1	Name2	Name3	Name4	KnownAs	Sex	DateOfBirt	DateOfJoi	Seniorit	SecretQuest	SecretAns	CrewPorta	BirthCity	BirthState	Salt	RuleSetI
[redacted]	1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	M	[redacted]	[redacted]	1	fine wine	[redacted]	0	[redacted]	[redacted]	[redacted]	NULL
[redacted]	0	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	M	[redacted]	[redacted]	1	test	[redacted]	0	[redacted]	[redacted]	[redacted]	NULL
[redacted]	6	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	M	[redacted]	[redacted]	0	Crew0006	[redacted]	6	[redacted]	[redacted]	[redacted]	NULL
[redacted]	28	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	F	[redacted]	[redacted]	0	Rating?	[redacted]	28	[redacted]	[redacted]	[redacted]	NULL
[redacted]	30	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	F	[redacted]	[redacted]	0	my name	[redacted]	30	[redacted]	[redacted]	[redacted]	NULL
[redacted]	32	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	M	[redacted]	[redacted]	0	Model	[redacted]	32	[redacted]	[redacted]	[redacted]	NULL
[redacted]	51	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	0	NULL	[redacted]	51	[redacted]	[redacted]	[redacted]	NULL
[redacted]	53	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	M	[redacted]	[redacted]	0	mum's nam	[redacted]	53	[redacted]	[redacted]	[redacted]	NULL
[redacted]	57	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	M	[redacted]	[redacted]	0	Football tea	[redacted]	57	[redacted]	[redacted]	[redacted]	NULL
[redacted]	61	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	M	[redacted]	[redacted]	373	NULL	[redacted]	61	[redacted]	[redacted]	[redacted]	NULL
[redacted]	62	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	M	[redacted]	[redacted]	0	NULL	[redacted]	62	[redacted]	[redacted]	[redacted]	NULL
[redacted]	63	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	M	[redacted]	[redacted]	393	NULL	[redacted]	63	[redacted]	[redacted]	[redacted]	NULL
[redacted]	64	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	M	[redacted]	[redacted]	0	NULL	[redacted]	64	[redacted]	[redacted]	[redacted]	NULL
[redacted]	71	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	F	[redacted]	[redacted]	0	What is hap	[redacted]	71	[redacted]	[redacted]	[redacted]	NULL

A .csv file of AirAsia's employee data with personal and work-related information
Source: DataBreaches.net

Cyber Incident Impacts Jeppesen's Flight Planning Tools

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



We are currently experiencing technical issues with some of our products, services and communication channels. We are working to restore functionality as soon as possible.

If you need support at this time, please reach out to us at support.jeppesen.com. Phone support is not available at this time.

This disruption is also impacting the receipt and processing of new NOTAMs and distribution of current NOTAMs. Flight Operators are reminded that the NOTAMs Offices (NoF) / Air Services Navigation Providers (ANSP) for the countries of departure, overflight, and arrival are alternative sources of NOTAMs.

The United States FAA and ICAO have access websites

https://notams.aim.faa.gov/notamSearch/ | https://www.icao.int/safety/istars/pages/notams.aspx

Notification by Jeppesen
Source: JEPPESEN

On 2 November 2022, A cybersecurity incident occurred at Jeppesen, Boeing subsidiary that provides navigation and flight planning tools. The Colorado-based firm experienced technical issues with the accuracy of some of their flight planning products and services. The extent of the disruptions was unclear but the incident affected the receipt and processing of current and new Notice to Air Missions (NOTAMs) — an industry term for notices filed with aviation authorities to alert pilots of potential hazards along a flight route. Jeppesen later successfully completed a full restoration of its systems after the incident.

Jeppesen later successfully completed a full restoration of its systems after the incident.

BAE Systems Launched a Technology to Reduce Cyber Attacks

Source: www.airforce-technology.com/, www.securityweek.com/

UK defence giant British Aerospace (BAE) Systems launched Viper Memory Loader Verifier II (MLV II), a system to protect F-16 fighter aircraft against potential cyberattacks. MLV II is used to load and verify software onto the fighter jet, ensuring that malicious software or files cannot get on the aircraft. The system also supports downloading of flight and fault data along with third-party application software. MLV II supports over 100 F-16 onboard systems, including flight and mission-critical components such as navigation, radar, engine control, communications, crash data recorders, and electronic warfare, mission and flight control.

Image source: https://www.baesystems.com/s

MLV II is used to load and verify software onto the fighter jet, ensuring that malicious software or files cannot get on the aircraft.

U.S. Police Planted a Smartphone Tracking Tool

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

According to a new investigation by the Associated Press (AP) it was revealed that several law enforcement agencies of Southern California and North Carolina have planted an obscure cellphone tracking tool. The tracking tool is named ‘Fog Reveal’ and sometimes it is used by law enforcement agencies without search warrants. The police have used 'Fog Reveal' tool to search hundreds of billions of records from 250 million mobile devices, and harnessed the data to create location analyses. 'Fog Reveal' use advertising identification numbers gathered from well-known smartphone apps that target ads based on a person’s movements and interests.

The tracking tool is named ‘Fog Reveal’ and sometimes it is used by law enforcement agencies without search warrants.

U.S. Bans Sales From Chinese Telecommunications Vendors

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

The United States government, through the Federal Communications Commission (FCC), has banned the sale of equipment from Chinese telecommunications and video surveillance vendor Huawei, Hytera, Hikvision, ZTE and Dahua due to 'unacceptable risks' to U.S. national security. The U.S. ban covers not only the parent companies but also their subsidiaries and affiliates as well.

Image source: https://www.fcc.gov/

Trends

Two Common File Types Used by Hackers

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

HP has observed that ZIP and RAR file types have overtaken the Office document files as most commonly used by the cyber threat actors to deliver malware. The research has found that in third quarter of 2022, 44 percent of malware was delivered inside archive files, registering a rise of 11 percent from previous quarter. HP has identified campaigns that combined the use of archive files with new HTML smuggling techniques to launch an attack. In this method the threat actors embed malicious archive files into HTML files to bypass email gateways. The archives are easy to encrypt thereby helping threat actors to conceal malware and evade sandboxes, web proxies, or email scanners. This makes the attacks difficult to detect, particularly when combined with HTML smuggling techniques. Recently QakBot and IcelD campaigns have used HTML files to direct users to fake online document viewers masquerading as Adobe.

The research has found that in third quarter of 2022, 44 percent of malware was delivered inside archive files, registering a rise of 11 percent from previous quarter.

Malware Bytes

New 'Maggie' Backdoor Targeting Microsoft SQL Servers

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

A new backdoor dubbed as ‘Maggie’, has been targeting Microsoft SQL (MSSQL) servers. Threat actors are deploying malware in the form of a signed Extended Stored Procedure (ESP) DLL file which is a type of extension used by MSSQL. The attacker must place the ESP file in a directory that the MSSQL server can access to execute the backdoor on the target server and needs valid credentials to load the ESP on the server. This backdoor has the ability to run commands and interact with files. The attackers can use this backdoor to gain a foothold into the compromised environment. It can be used to enable network-related functionality, including a Socks5 proxy server, TermService and port forwarding, which allows the backdoor to act as a bridge head into the server’s network environment. Maggie can also launch brute force attacks against other MSSQL servers, targeting admin accounts to add a hardcoded backdoor user. It also supports simple TCP redirection which allows it to redirect incoming connections to a previously defined IP and port.

Threat actors are deploying malware in the form of a signed Extended Stored Procedure (ESP) DLL file which is a type of extension used by MSSQL.

New Malware Targets Windows, Mac and Linux Systems

Source: https://thehackernews.com/

An attack framework dubbed as ‘Alchimist’ and its associated Remote Access Trojan (RAT) is targeting Windows, Linux and macOS systems. The attack framework provides a web interface which allows operators to generate and deploy malicious payloads, establish remote connections, execute code on the compromised machines and take screenshots. The attack framework and Insekt RAT that it implants on compromised systems, are implemented in GoLang. Other post-exploitation tools including a reverse proxy targeting macOS (frp), a custom backdoor and other various off-the-shelf tools such as psexec, netcat, and fscan, have been used in this campaign. Alchimist stores resources for functioning as a Command & Control (C&C) server in GoLang-based assets and allows users to generate PowerShell and wget code snippets to Windows and Linux. The RAT also checks the system’s Internet connectivity, supports shellcode execution, port IP scanning, proxy connections and SSH manipulation, can list the ‘.ssh’ directory on Linux, and can execute arbitrary commands on the operating system’s shell.

The attack framework provides a web interface which allows operators to generate and deploy malicious payloads, establish remote connections, execute code on the compromised machines and take screenshots.

New 'Black Lotus' UEFI Rootkit with APT-Level Capabilities

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

A new powerful Windows UEFI rootkit, dubbed as ‘Black Lotus’ is promoting on underground cyber-criminal forums. Black Lotus supports a full set of backdoor capabilities, which could be used to potentially target IT and OT environments. It brings APT capabilities to malicious actors in the threat landscape. The availability of this rootkit in the threat landscape represents a serious threat for Critical organisations due to its evasion and persistence capabilities. The malware supports anti-virtualisation, anti-debugging and code obfuscation. Black Lotus has the ability to disable security solutions, including BitLocker, Hypervisor-protected Code Integrity (HVCI) and Windows Defender. The rootkit is able to bypass security defenses like User Access Control (UAC) and Secure Boot. It is also able to load unsigned drivers used to perform a broad range of malicious activities.

The malware supports anti-virtualisation, anti-debugging and code obfuscation. Black Lotus has the ability to disable security solutions, including BitLocker, Hypervisor-protected Code Integrity (HVCI) and Windows Defender.

POLONIUM Targets Israel with Creepy Malware

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

POLONIUM, an Advanced Persistent Threat (APT) group is targeting various organisations in Israel. The threat group is using multiple custom backdoors.

- CreepyDrive is a PowerShell backdoor which abuses Dropbox, Mega and OneDrive for Command & Control (C2) communications. CreepyDrive uses the Dropbox and OneDrive HTTP API to access the cloud storage.
- CreepySnail is another PowerShell backdoor that sends HTTP requests to C2 server to receive and execute the PowerShell commands.

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

- DeepCreep backdoor reads commands from a text file stored in Dropbox accounts and can upload or download files to and from those accounts.
- MegaCreep bakdoor reads and executes commands from a text file stored in Mega cloud storage.
- FlipCreep, TechnoCreep & PapaCreep backdoor can receive and execute commands from C2 servers.

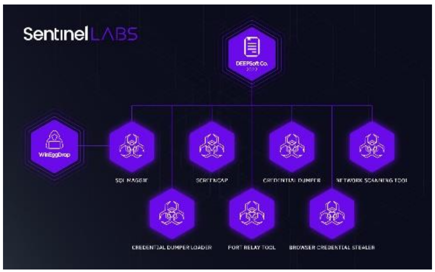
DeepCreep backdoor reads commands from a text file stored in Dropbox accounts and can upload or download files to and from those accounts.

POLONIUM uses several other modules on top of these backdoors, including reverse shell modules and a module for creating a tunnel. The group uses custom tools for taking screenshots, spying via the webcam, logging keystrokes, opening reverse shells, exfiltrating files and more.

WIP19 Espionage Targets IT Service Providers and Telcos

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

Threat cluster tracked as WIP19 has been targeting Telecommunications and IT service providers. The threat actor has been exploiting stolen legitimate digital certificate issued by a company "DEEPSoft", to sign several malwares including SQLMaggie, ScreenCap and a credential dumper. The SQLMaggie malware dropped on victim networks masquerades as a legitimate DLL containing extended stored procedure functions for an MSSQL Server. After registering the DLL into the MSSQL server, the threat actor gets the ability to fully control the server machine and use backdoor to conduct reconnaissance in the internal network. ScreenCap is used for Keylogger & Screen Recording.



Relationship between the malware, certificates, and creators

'Spyder Loader' Malware Targeted Organisations in Hong Kong

Source: https://thehackernews.com/

It has been observed that espionage actor Winnti aka APT41, Barium, Bronze Atlas and Wicked Panda, is breaching government organisations in Hong Kong aiming to collect intelligence. It remained undetected in some cases. The infection chain starts with spear-phishing emails with malicious attachments to initially break into the victims' networks. The threat actor has been using custom malware backdoor called Spyder Loader in its latest CuckooBees operation. The spyder is being used for targeted attacks on information storage systems, executing mischievous payloads, collecting information about corrupted devices, coordinating script execution and C2 server communication. This campaign is using other post-exploitation tools, such as Mimikatz and a trojanized zlib DLL module. This DLL Module has the ability to communicate with Command & Control (C2) server or load an arbitrary payload.

The infection chain starts with spear-phishing emails with malicious attachments to initially break into the victims' networks.

Self-Replicating Malware Used by Cyberspies

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

UNC4191 group has been observed using self-replicating malware on USB drives to infect targets. The cyberespionage group, UNC4191 is deploying legitimately signed binaries to side-load malware. The threat actor has been using malware families such as the Mistcloak launcher, the Darkdew dropper and the Bluehaze launcher. The attackers are also deploying the NCAT command-line networking utility for file download and upload purposes and a reverse shell on the target machine. Reverse shell is used to achieve backdoor access to the compromised system. The malware self-replicates by infecting new removable drives that are plugged into a compromised system, which allows the malicious payloads to propagate to additional systems and potentially collect data from air-gapped systems.

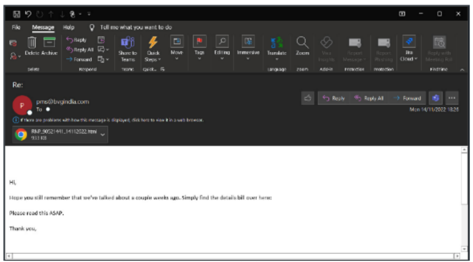
Image source: https://www.hackread.com/

The attackers are also deploying the NCAT command-line networking utility for file download and upload purposes and a reverse shell on the target machine.

QBot Phishing Abuses Windows Control Panel EXE to Infect Devices

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

It has been observed that Phishing emails are using a DLL hijacking flaw in the Windows Control Panel to distribute the QBot malware. DLL hijacking is a common attack method that takes advantage of how Dynamic Link Libraries (DLLs) are loaded in Windows. The Windows malware QBot, also known as Qakbot, started as a banking trojan but evolved into a full-featured malware dropper. Ransomware gangs including Black Basta, Egregor, and Prolock, are also using the malware to gain initial access to target's networks. The malware is downloading additional payloads such as Brute Ratel or Cobalt Strike. Brute Ratel and Cobalt Strike are post-exploitation toolkits that threat actors use to gain remote access to organisations networks which leads to data theft and ransomware attacks.



Re:

pms@bvgindia.com
To

Mon 14/11/2022 18:26

If there are problems with how this message is displayed, click here to view it in a web browser.

RNP_90521411_14112022.html
933 KB

Hi,

Hope you still remember that we've talked about a couple weeks ago. Simply find the details bill over here:

Please read this ASAP.

Thank you,

QBot phishing email in new campaign

APT Groups Use Impacket and Exfiltration Tool

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

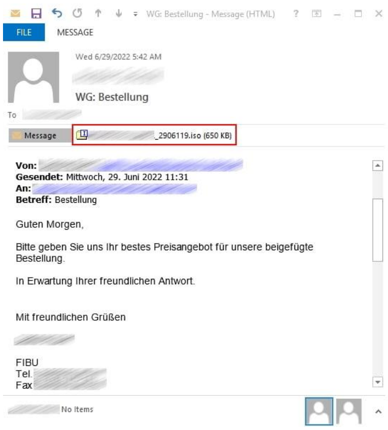
Cybersecurity and Infrastructure Security Agency (CISA) discovered that Advanced Persistent Threat (APT) actors were using Impacket and Exfiltration tool to invade a Defence Industrial Base (DIB) sector organisation's enterprise network. The APT actors used an open-source toolkit called Impacket, a python toolkit for programmatically constructing and manipulating network protocols, to gain their foothold within an organisation's environment and further compromise the network. The APT groups employed a custom exfiltration tool called CovalentStealer to exfiltrate sensitive files. The task of CovalentStealer is to identify file shares on a system, categorise the files, and upload the files to a remote server. The actors used Command Shell to learn about the

The APT groups employed a custom exfiltration tool called CovalentStealer to exfiltrate sensitive files.

organisation's environment and to collect sensitive data for exfiltration. CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) recommend that DIB sector and other critical infrastructure organisations should implement mitigations steps to ensure that they are managing and reducing the impact of cyber threats to their networks.

DarkTortilla Malware

South Zone, NCIIPC



Wed 6/29/2022 5:42 AM
[redacted]
WG: Bestellung
To [redacted]

Message [redacted]_2906119.iso (650 KB)

Von: [redacted]
Gesendet: Mittwoch, 29. Juni 2022 11:31
An: [redacted]
Betreff: Bestellung

Guten Morgen,

Bitte geben Sie uns Ihr bestes Preisangebot für unsere beigefügte Bestellung.

In Erwartung Ihrer freundlichen Antwort.

Mit freundlichen Grüßen

[redacted]

FIBU
Tel. [redacted]
Fax

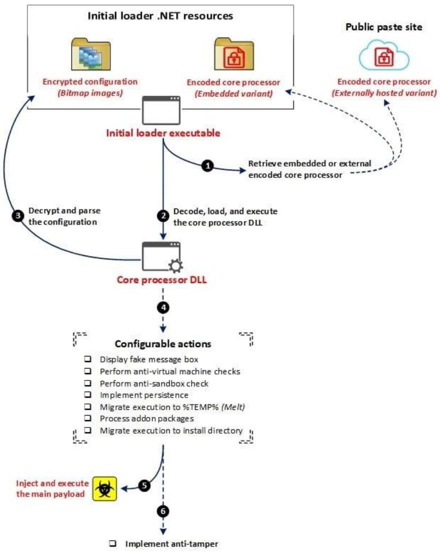
[redacted] No Items

DarkTortilla malspam containing malicious archive attachment

DarkTortilla is a complex and configurable .NET-based evasive cryptor active since August 2015. The malware features like high degree of configurability and robust anti-tamper controls making the detection, analysis and removal harder or highly challenging. The malware is very sophisticated in nature due to execution of its payload entirely in memory. Malware is distributed to users through spam emails with malicious attachments. Attackers use .iso, .zip, .img, .dmg, .doc, and .tar files to spread the DarkTortilla malware. In some instances, the threat actor has also created various phishing websites to deliver the malware.

Attackers have been using the malware to distribute information stealers used to get the keystrokes, data from web browsers, other installed applications, extract data. Most recently, it has been used largely to distribute malware such as Remote Access Trojans (RATs) AgentTesla, AsyncRAT, NanoCore, etc., and targeted payloads such as Metasploit to get remote access of the infected system. This malware is capable of delivering numerous "addon packages". Some of them are additional malicious payloads, documents, and executables files. It is also able to access the microphone and webcam, capture screenshots and perform other actions like upload, download.

Modus Operandi: User who clicks the link to the spoofed photo grid website ends up downloading of a malicious file. That phishing website installs a malicious zip file named "photogridInstaller.zip", when they click on the "Get Photo grid" button. The .zip additionally holds a malicious cabinet file, "photogridInstaller.ch9uagh7baddwd8jse1ovd6g06.exe" masking itself as a photo grid executable. The .exe file is an archive file which when executes, gives a .NET-based file in the temp folder of the system.


Initial loader .NET resources
Encrypted configuration (Bitmap images)
Encoded core processor (Embedded variant)
Public paste site
Encoded core processor (Externally hosted variant)
Initial loader executable
1 Retrieve embedded or external encoded core processor
2 Decode, load, and execute the core processor DLL
3 Decrypt and parse the configuration
Core processor DLL
4
Configurable actions
❑ Display fake message box
❑ Perform anti-virtual machine checks
❑ Perform anti-sandbox check
❑ Implement persistence
❑ Migrate execution to %TEMP% (Melt)
❑ Process addon packages
❑ Migrate execution to install directory
Inject and execute the main payload
5
6
❑ Implement anti-tamper

High-level execution flow for DarkTortilla infection

The malware then downloads a DLL file into the system's memory, which acts as main or final payload and can execute malicious activities in the system. The files downloaded from the phishing websites have diverse infection techniques, by providing a sophisticated platform to the threat actor capable of modifying the binary.

Best Practices: A few basic critical cybersecurity best practices that create the first line of defence against attackers are as under:

- Download software from certified pages and genuine stores only.
- Downloads from third-party downloaders, P2P networks (e.g., torrent clients) should be avoided.
- Double-check emails before opening their contents.
- Refrain from opening suspicious links and attachments in email without verifying their authenticity.
- Do not trust advertisements.
- Configure regular scans and monitor security settings
- Limit file-sharing.
- Use admin accounts when absolutely necessary.
- Implement email security and spam protection.
- Keep operating system and other installed programs updated.

Always update operating system and installed programs timely.

References:

[1] https://www.secureworks.com/research/darktortilla-malware-analysis

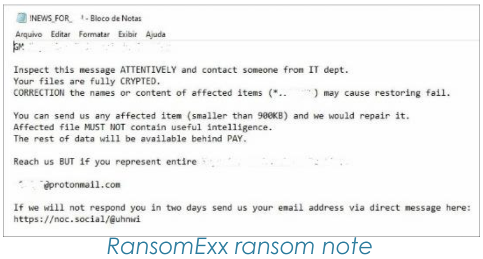
[2] https://malpedia.caad.fkie.fraunhofer.de/details/win.darktortilla

[3] https://www.sciencedirect.com/topics/computer-science/detecting-malware

RansomExx Ransomware

South Zone, NCIIPC

RansomExx ransomware is an emerging threat within the cyber world that researchers are working upon after its initial discovery in 2018 under the name "Defray". Since then, it has become a worldwide concern and has impacted many enterprises in various countries in Asia, Europe, America. Recently to expand their attack scope, the latest updates are being added to the ransomware in Rust Language in order to get low detection rates and to make its reverse engineering difficult. This ransomware is using fast and safe file encryption methods.



```
GM[redacted]

Inspect this message ATTENTIVELY and contact someone from IT dept.
Your files are fully CRYPTED.
CORRECTION the names or content of affected items (*..[redacted]) may cause restoring fail.

You can send us any affected item (smaller than 900KB) and we would repair it.
Affected file MUST NOT contain useful intelligence.
The rest of data will be available behind PAY.

Reach us BUT if you represent entire [redacted]

[redacted]@protonmail.com

If we will not respond you in two days send us your email address via direct message here:
https://noc.social/@uhnwi
```

RansomExx ransom note
Source: Bleeping Computer

Targets of RansomExx: Threat actors have used this ransomware to target wide range of large businesses, educational institutions, enterprises and critical infrastructure organisations including transport, manufacturers, healthcare and medical industries. This ransomware is extremely active in the manufacturing and banking sectors.

Threat actors have used this ransomware to target wide range of large businesses, educational institutions, enterprises and critical infrastructure organisations including transport, manufacturers, healthcare and medical industries.

Modus Operandi: RansomExx has the capability to encrypt files/data on windows and also on Linux operating systems. This ransomware is usually delivered as file less malware. It is hard for security solutions to detect this type of ransomware because it is executed in memory without touching the hard drive. Once the RansomExx is executed, each encrypted file has ".txd" extension appended to filenames. For example, a file named "cri.jpg" would be renamed to "cri.jpg.txd", "decr.jpg" to "decr.jpg.txd", and so on.

> *RansomExx has the capability to encrypt files/data on windows and also on Linux operating systems. This ransomware is usually delivered as file less malware.*

A ransom message appears, within a text file in all folders that contain encrypted files. The message also offers free decryption of one encrypted file for proving the legitimacy of the attacker. Victims are then forced to send an email to the given address to purchase decryptor software by paying hefty amount of money.

Best practices: Ransomware attacks are very difficult to prevent, as these spread often through social engineering mechanisms. However, the following practices may help to reduce the risk of RansomExx attack.

- Backups: The risk of ransomware may be reduced by implementing a backup plan to maintain numerous copies of sensitive data and servers both on- and off- site in a completely separate, segmented, and safe location and also ensure that all backup data is encrypted.
- Authentication: The risk of ransomware may be reduced by implementing multifactor authentication wherever possible to provide extra layer of security particularly the accounts that access critical systems.
- System Hardening: The risk of ransomware may be reduced by hardening of firmware, software and all operating systems periodically to reduce security risk by eliminating potential attack vectors and abridging the system's attack surface.
- Audit: The risk of ransomware may be reduced by conducting the audit of all user accounts and configure access controls according to the principle of least privilege.
- The risk of ransomware may be reduced by disabling all unused ports and following basic cyber hygiene.
- The risk of ransomware may be reduced by conducting regular cybersecurity awareness training for the end users to stay across current threats.

> *The risk of ransomware may be reduced by conducting regular cybersecurity awareness training for the end users to stay across current threats.*

References:

[1] https://securelist.com/ransomexx-trojan-attacks-linux systems/99279/

[2] https://www.pcrisk.com/removal-guides/19847-ransomexx-ransomware

[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.ransomexx

Ransomware Quarterly Stats (Oct-Dec 2022)

Month	No. of advisory issued	No. of IOCs
October	5	94
November	6	78
December	9	220
Total	20	392

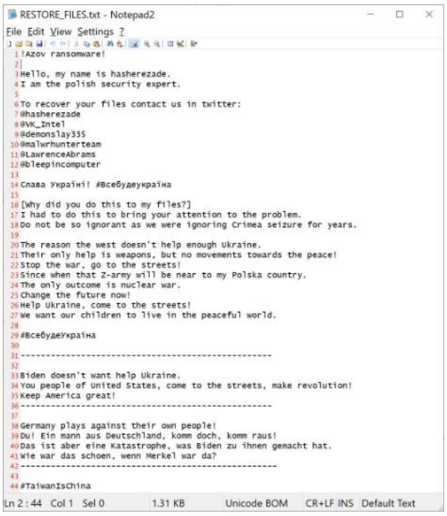
Quarterly Ransomware Brief

Knowledge Management Team, NCIIPC

Ransomware Tactics, Techniques and Procedures (TTPs) continued to evolve exhibiting ransomware threat actors' with growing technological sophistication. Ransomware actors are using multiple tools and techniques to obtain initial access such as phishing emails, Drive-By Downloads from a compromised Website, Remote Desktop Protocol (RDP), third parties & Managed Service

Providers (MSP), supply chain compromise and USB/Removable Media and through Dark Web Forum. NCIIPC has issued multiple ransomware advisory during Q4 2022 quarter to protect Critical Information Infrastructures (CIIs)/ Protected Systems (PSs). Some of the prominent ransomware in this quarter are as follows:

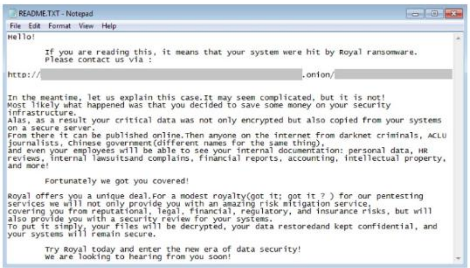
The Azov Ransomware continues to be heavily distributed worldwide and now it is proven to be a data wiper that intentionally destroys victim's data and infects other programs. In October 2022, a threat actor began distributing malware called 'Azov Ransomware' through cracks and pirated software that pretended to encrypt victim's files.


RESTORE_FILES.txt - Notepad2
File Edit View Settings ?
Ln 2 : 44 Col 1 Sel 0 1.31 KB Unicode BOM CR+LF INS Default Text

```
!Azov ransomware!

Hello, my name is hasherezade.
I am the polish security expert.

To recover your files contact us in twitter:
@hasherezade
@VK_Intel
@demonslay335
@malwrhunterteam
@LawrenceAbrams
@bleepincomputer

Слава Україні! #Всебудеукраїна

[Why did you do this to my files?]
I had to do this to bring your attention to the problem.
Do not be so ignorant as we were ignoring Crimea seizure for years.

The reason the west doesn't help enough Ukraine.
Their only help is weapons, but no movements towards the peace!
Stop the war, go to the streets!
Since when that Z-army will be near to my Polska country.
The only outcome is nuclear war.
Change the future now!
Help Ukraine, come to the streets!
We want our children to live in the peaceful world.

#ВсебудеУкраїна

-----------------------------------------------------

Biden doesn't want help Ukraine.
You people of United States, come to the streets, make revolution!
Keep America great!
-----------------------------------------------------

Germany plays against their own people!
Du! Ein mann aus Deutschland, komm doch, komm raus!
Das ist aber eine Katastrophe, was Biden zu ihnen gemacht hat.
Wie war das schoen, wenn Merkel war da?
------------------------------------------------------

#TaiwanIsChina
```

'Azov Ransomware' data wiper note to victims

Royal Ransomware is a 64-bit windows executable written in C++. This ransomware appears to use the Open SSL library to encrypt files to the AES standard and all encrypted files are renamed and given a .royal file extension. Royal Ransomware group's object is to gain access to a victim's environment, encrypt their data and extort a ransom to return access to any files touched.



```
Hello!

        If you are reading this, it means that your system were hit by Royal ransomware.
        Please contact us via :

http://[redacted].onion/[redacted]


In the meantime, let us explain this case.It may seem complicated, but it is not!
Most likely what happened was that you decided to save some money on your security
infrastructure.
Alas, as a result your critical data was not only encrypted but also copied from your systems
on a secure server.
From there it can be published online.Then anyone on the internet from darknet criminals, ACLU
journalists, Chinese government(different names for the same thing),
and even your employees will be able to see your internal documentation: personal data, HR
reviews, internal lawsuitsand complains, financial reports, accounting, intellectual property,
and more!

        Fortunately we got you covered!

Royal offers you a unique deal.For a modest royalty(got it; got it ? ) for our pentesting
services we will not only provide you with an amazing risk mitigation service,
covering you from reputational, legal, financial, regulatory, and insurance risks, but will
also provide you with a security review for your systems.
To put it simply, your files will be decrypted, your data restoredand kept confidential, and
your systems will remain secure.

        Try Royal today and enter the new era of data security!
        We are looking to hearing from you soon!
```

Royal ransom note

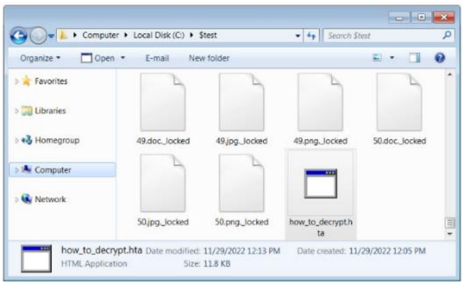
The new 'AXLocker' ransomware family is not only encrypting victim's files and demanding a ransom payment but also stealing the Discord, a VoIP and instant messaging social platform, accounts of infected users. AxLocker uses AES algorithm and it does not append extension to filename on the encrypted files, so they appear with their normal names. If you encounter AXLocker ransomware on your computer, it is recommended to change your Discord password immediately.

The new 'AXLocker' ransomware family is not only encrypting victim's files and demanding a ransom payment but also stealing the Discord accounts of infected users.

QBot also known as Qakbot is a Windows malware that started as a banking Trojan but evolved into a full featured malware dropper. Ransomware gangs like Black Basta, Prolock, and Egregor use QBot malware to gain initial access to corporate networks. This remote access leads to corporate data theft and ransomware attacks. In July 2022 it was discovered that threat actors were exploiting a DLL hijacking vulnerability in the windows 7 calculator to install QBot malware.

RansomBoggs Ransomware targeted several Ukrainian organisations. The malware is written in .NET and its deployment is similar to previous attacks attributed to Sandworm. The RansomBoggs activity is said to employ a Powershell script to distribute the ransomware almost similar to the one used in the Industroyer2 malware attack.

Trigona ransomware operation launched a new Tor negotiation site in Oct 2022. Trigona encrypts all files on a device except some files in Windows and Program files folders. Trigona uses ._locked extension for encrypted files. The ransomware also embeds the encrypted decryption key, campaign ID and victim ID in the encrypted files.



how_to_decrypt.hta Date modified: 11/29/2022 12:13 PM Date created: 11/29/2022 12:05 PM
HTML Application Size: 11.8 KB

Files encrypted by Trigona

References:

[1] https://www.bleepingcomputer.com/news/security/azov-ransomware-is-a-wiper-destroying-data-666-bytes-at-a-time/

[2] https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware

[3] https://www.bleepingcomputer.com/news/security/new-ransomware-encrypts-files-then-steals-your-discord-account/

[4] https://www.bleepingcomputer.com/news/security/qbot-phishing-abuses-windows-control-panel-exe-to-infect-devices/

[5] https://thehackernews.com/2022/11/russia-based-ransomboggs-ransomware.html

[6] https://www.bleepingcomputer.com/news/security/trigona-ransomware-spotted-in-increasing-attacks-worldwide/

Learning

Threats and Indicators of a Misaligned Saboteur

Source: https://www.securonix.com/

Insider in a technical role who becomes misaligned with their organisation and decides to retaliate by sabotaging resources impacts the confidentiality, integrity, or availability with respect to the organisational mission. The common indicators of an Insider Sabotage are:

Insider in a technical role who becomes misaligned with their organisation and decides to retaliate by sabotaging resources impacts the confidentiality, integrity, or availability with respect to the organisational mission.

- 84% claim that they were motivated by revenge, while 12% claimed that they were acting for personal gain.
- In 80% of the incidents, the threat actors have broken rules or policies or engaged in interpersonal disputes before their attacks.
- 90% of threat actors tried to obfuscate their actions.
- The majority of attacks occurred outside of normal working hours and used remote access.

Securing Domain Controllers Against Attack

Source: https://learn.microsoft.com/

Domain controller is a server that process requests for authentication from users within a LAN/network. It provides physical storage for the Active Directory Domain Services (AD DS) database along with services and data that allow enterprises to effectively manage their servers, workstations, users and applications. Compromising a domain controller provide direct path to destruction of member servers, workstations and Active Directory. Therefore, domain controller should be secured separately than the general infrastructure.

Compromising a domain controller provide direct path to destruction of member servers, workstations and Active Directory.

Physical Security for Domain Controller:

- Physical Domain Controllers should be installed in dedicated secure racks from the general server.
- Virtual Domain Controllers should run on separate physical hosts than other virtual machines in the environment.
- Domain Controller operating systems should run on the newest version of Windows Server.

Security Configuration of Domain Controllers:

- Group Policy Objects that link to all domain controllers should be configured to allow only authorised RDP connections.
- Patching of Domain Controllers and other critical infrastructure components should be separated from general infrastructure.
- Launching web browsers and general Internet access to and from domain controllers should be strictly controlled.
- Perimeter firewalls should be configured to block outbound connections from domain controllers to the Internet.

Patching of Domain Controllers and other critical infrastructure components should be separated from general infrastructure.

Securing the Software Supply Chain: Recommended Practices

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

Software Supply Security is the act of securing the components, activities and practices involved in the creation and deployment of software. Unmitigated vulnerabilities in the software supply chain pose a significant risk to organisations. It is the responsibility of organisations to establish software supply chain security practices to mitigate risks.

Unmitigated vulnerabilities in the software supply chain pose a significant risk to organisations. It is the responsibility of organisations to establish software supply chain security practices to mitigate risks.

1. Secure product criteria and management

- Architecture and design documents: Architecture and design documents should be based on customer and marketing requirements that have been gathered, correlated and prioritised.
- The development team: Members of the development team should be trained and qualified to perform the security

development tasks outlined in the architecture and high-level design document.

Development organisations should employ dedicated systems that download, scan, and perform recurring checks of open source libraries for new versions, updates, and known or new vulnerabilities.

- Threat models: All code and systems involved within the build pipeline should be reviewed on an ongoing basis against the associated threat model.
- Security test plans: An impartial Quality Assurance (QA) individual, team, or an impartial entity with QA expertise should define and implement security test plans.
- Release criteria: The management team should establish, manage, and apply release criteria and evaluate whether the product satisfies the criteria.
- Product support and vulnerability handling policies: The management team defines the product support and vulnerability handling policies and procedures as they address the entire lifecycle of the product from conception to end of life (EOL).

2. Develop Secure Code

- Modification or Exploitation of Source Code by Insiders: Software development group managers should ensure that the development process prevents the intentional and unintentional injection of malicious code or design flaws into production code.

Development managers should ensure that the components and software integrated into the delivered product is tested within the integrated environment for which it will be deployed.

- Open-Source Management Practices: Development organisations should employ dedicated systems that download, scan, and perform recurring checks of open-source libraries for new versions, updates, and known or new vulnerabilities.
- Secure Development Practices: Managers of a software development group should ensure that the development process used to generate, test, and preserve source code are accomplished using well-defined and secure practices.
- Code Integration: Development managers should ensure that the components and software integrated into the delivered product is tested within the integrated environment for which it will be deployed.
- Defect/Vulnerability Customer Reported Issue: Managers of software development group should ensure that the software they develop is free of high-risk known defects and vulnerabilities.

3. Verify Third-Party Components

- Third-Party Binaries: Binary scanning and software composition analysis tools can often detect unknown files and the open-source components contained in binary packages.

- Selections and Integration: Before the integration of third-party components, each component must be evaluated for the potential security risk that might be associated with it.

- Obtain Components from a Known and Trusted Supplier: When considering the selection of a third-party component, care should be taken to build a relationship with a known and trusted supplier that has a proven record for secure coding practices and quality delivery of their components.

- Software Bill of Materials (SBOM): The details of an integrated third-party component should be reported in an SBOM for the product developed to easily validate approved components and identify the presence of vulnerable components when defects are discovered.

The details of an integrated third-party component should be reported in an SBOM for the product developed to easily validate approved components and identify the presence of vulnerable components when defects are discovered.

4. Harden the Build Environment

- Build Chain Exploits: The build pipeline infrastructure includes all systems that come in contact with the development and build process such as source code repositories, engineering workstations, and deployment servers for both on-premise machines and those hosted in the cloud.

- Exploited Signing Server: A threat actor could impersonate a target by compromising the code-signing service, using the signing system to sign compromised components or products.

Binary software composition analysis tools can investigate what exactly is included in the final deliverables and identify potential issues in the final packages.

5. Deliver Code

- Final Package Validation: Binary software composition analysis tools can investigate what exactly is included in the final deliverables and identify potential issues in the final packages.

- Potential Tactics to Compromise the Software Packages and Updates: The package may be compromised while going through the distribution system from the supplier to the customer.

- Compromises of the Distribution System: Attacks to the distribution system include compromising the repository to introduce malware into the packages stored in the repository.

Internet Information Services (IIS) Malware

South Zone, NCIIPC

Internet Information Services (IIS) is the web server developed by Microsoft which runs on the Microsoft .NET platform. This web server has been an essential fragment of the Windows NT family that runs on Windows operating systems to support HTML pages/files. All IIS modules, operate in the same phases. Malicious IIS Modules are the perfect backdoors. Once installed, they will intercept the HTTP requests coming to the compromised IIS server and later use the compromised server for further malicious activities. The IIS Malware processes the requests for logs (network) and other sensitive information. IIS malware modules are often very difficult to detect as these are being installed in the same path and using the exact structure as legitimate modules. These malicious modules provide a long-term and durable persistence mechanism to the attackers. After installation, malicious IIS modules allow attackers to fetch credentials from server and gather confidential information from the malicious network and infected devices. Functions of Malicious IIS modules are:

Malicious IIS Modules are the perfect backdoors. Once installed, they will intercept the HTTP requests coming to the compromised IIS server and later use the compromised server for further malicious activities.

IIS malware modules are often very difficult to detect as these are being installed in the same path and using the exact structure as legitimate modules.

- Installing backdoor,
- Information theft,
- Traffic convenience by neutering protocol responses,
- Proxies to display the compromised servers into traffic relays between diverse malware programs.

Preventing compromise of IIS Servers: Organisations or entities must ensure to follow security practices to defend their servers. Indeed, many malware attacks take advantage of the software vulnerabilities in commonly used operating systems, applications and browsers. Following are some of the recommendations:

- Passwords should be strong and unique.
- Use dedicated accounts only for managing the IIS server.
- Implement multifactor authentication for all accounts.
- Usage of dedicated accounts should be monitored.
- Restrict access to virtual directories of IIS modules and regularly review the config files and bin folders.
- Constantly patch and update outdated operating system (OS) to make it compatible with various latest software, applications and devices.

Restrict access to virtual directories of IIS modules and regularly review the config files and bin folders.

- Usage of firewall or endpoint security solution should be managed and monitored cautiously.

- Install IIS modules from trusted sources only.

- To confirm the authenticity of installed IIS modules signed by a trusted provider, user should check the configuration file regularly.

- Periodically apply latest security updates.

- Keep antivirus & threat protections enabled.

To confirm the authenticity of installed IIS modules signed by a trusted provider, user should check the configuration file regularly.

References:

[1] Mike Volodarsky, “IIS Modules Overview”, Microsoft, 2007. Available: https://docs.microsoft.com/en-us/ iis/get-started/introduction-to-iis/iis-modules-overview.

[2] Josh Grunzweig, “The Curious Case of the Malicious IIS Module”, Trustwave, 2013. Available: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-curious-case-of-the-malicious-iis-module/.

[3] Anton Cherepanov, Robert Lipov sky, “Grey Energy: Updated arsenal of one of the most dangerous threat actors” ESET, 2018. https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenaldangerous-threat-actors/.

Vulnerability Watch

Critical Vulnerabilities in Abode Systems

Source: https://nvd.nist.gov/

Image source: https://www.adobe.com/in/

Critical OS command injection vulnerabilities with CVSS v3 score of 10.0 have been discovered in XCMD testWifiAP functionality of Abode Systems iota All-In-One Security Kit 6.9X and 6.9Z. Attacker can trigger these vulnerabilities by sending sequence of malicious commands. The CVE Id for these vulnerabilities is CVE-2022-33195, CVE-2022-33194, CVE-2022-33193 and CVE-2022-33192.

Critical Vulnerability in Honeywell

Source: https://nvd.nist.gov/

Image source: https://process.honeywell.com/

Honeywell industrial automation with Experion Process Knowledge System (PKS) provides enterprise-wide solution to business requirement and asset management. The Experion Process Knowledge System C200, C200E, C300 and ACE Controllers were found to be vulnerable to unrestricted file uploads. The CVE Id for this vulnerability is CVE-2021-38397 with CVSS v3 score of 10.0. This critical vulnerability allows attacker to remotely execute arbitrary code and cause a denial-of-service condition.

Mitsubishi Electric's Security Updates

Source: https://www.cisa.gov/uscert/ics/advisories/icsa-22-335-01

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

An improper input validation vulnerability has been found in Mitsubishi Electric. The CVE ID for this vulnerability is CVE-2022-40265 with CVSS v3 score of 8.6. The affected products of Mitsubishi Electric MELSEC iQ-R Series are RJ71EN71 (Firmware version "65" and prior) and R04/08/16/32/120ENCPU (Network part firmware version "65" and prior). Successful exploitation of this vulnerability allows remote unauthenticated attacker to cause a Denial-of-Service (DoS) attack on the target. To mitigate the vulnerability, it is required to update firmware version to "66" or later. It is recommended that user should use product within a Local Area Network (LAN), use IP filter function to restrict the accessible IP addresses, block access from untrusted networks and hosts through firewall.

Successful exploitation of this vulnerability allows remote unauthenticated attacker to cause a Denial-of-Service (DoS) attack on the target.

Vulnerability in Horner Automation's Equipment

Source: https://www.cisa.gov/uscert/ics/advisories/icsa-22-335-02

Multiple vulnerabilities have been found in Horner Automation Remote Compact Controller (RCC) 972. The vulnerabilities are Inadequate Encryption Strength (CVE-2022-2640) having CVSS v3 score of 7.5, Use of Hard-coded Cryptographic Key (CVE-2022-

2641) having CVSS v3 score 9.8, Excessive Reliance on Global Variables (CVE-2022-2642) having CVSS score of 7.5. The config-files of equipment with firmware version 15.40 are encrypted with weak XOR encryption vulnerable to reverse engineering which allows attacker to obtain credential to run services such as File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP). The firmware has a static encryption key on the device, which allows attacker to perform unauthorised changes to the device. The firmware also contains global variables which allows attacker to read out sensitive values and variable keys from the device. It is recommended to mitigate this vulnerability the firmware be updated to version 15.60 or later.

Image source: https://hornerautomation.com/

Critical Vulnerability in vm2 sandbox

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-36067

Critical vulnerability (CVE-2022-36067) with CVSS v3 score of 10.0 has been found in vm2 sandbox. Vm2 is a sandbox that run untrusted code with whitelisted Node's built-in modules. NPM package of vm2 versions prior to 3.9.11 are affected with this vulnerability. Successful exploitation of this vulnerability allows disclosure of sensitive information, addition or modification of data and Denial of Service (DoS). This vulnerability is patched in the version 3.9.11.

Successful exploitation of this vulnerability allows disclosure of sensitive information, addition or modification of data and Denial of Service (DoS).

Critical Vulnerability in ETIC Telecom Remote Access Server

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-40981

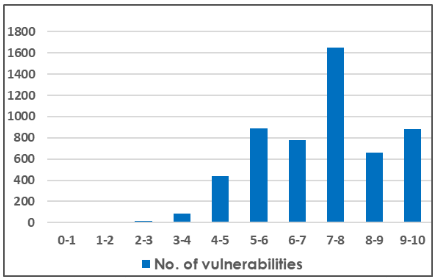
ETIC Telecom RAS is a tool, that facilitates in Remote control and monitoring. It provides secure machine remote maintenance from a PC or a smartphone. A critical vulnerability CVE-2022-40981 with CVSS Score 10.0 has been found in ETIC Telecom Remote Access Server. All versions of ETIC Telecom Remote Access Server (RAS) 4.5.0 and prior is vulnerable to malicious file upload. Adversary can store malicious file on the server, after exploiting the vulnerability. The vulnerability allows overriding sensitive and useful existing files on the filesystem, fill the hard disk to full capacity, compromise the affected device or computers with administrator level privileges connected to the affected device.

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

Quarterly Vulnerability Analysis Report

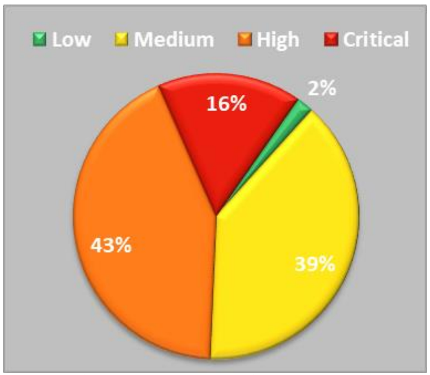
KMS Team, NCIIPC

During the last quarter of 2022, a total of 5414 vulnerabilities have been observed, out of which majority of vulnerabilities are of High Severity having score ranging from 7-9. 16 percent of total vulnerabilities reported were of Critical severity. Google, Microsoft, Apple, Linux and Fedoraproject were the top five vendors having 23% share of total reported vulnerabilities.



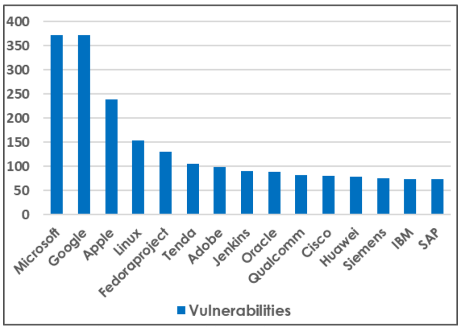
Severity-wise number of vulnerabilities

Severity	CVSSv3 Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Sep'22	Oct'22	Nov'22		
Low	0-1	0	0	0	0	106
	1-2	0	0	0	0	
	2-3	12	3	4	19	
	3-4	25	36	26	87	
Medium	4-5	143	123	176	442	2112
	5-6	340	294	255	889	
	6-7	249	262	270	781	
High	7-8	689	542	422	1653	2312
	8-9	253	196	210	659	
Critical	9-10	314	305	265	884	884
Total		2025	1761	1628		5414



Severity-wise share of vulnerabilities

S. No.	Vendor	No. of Vulnerabilities			Total
		Sep'22	Oct'22	Nov'22	
1.	Google	163	96	112	371
2.	Microsoft	146	127	98	371
3.	Apple	125	20	93	238
4.	Linux	50	62	41	153
5.	Fedoraproject	87	27	16	130
6.	Tenda	39	34	33	106
7.	Adobe	66	33	0	99
8.	Jenkins	32	35	24	91
9.	Oracle	4	80	5	89
10.	Qualcomm	45	22	15	82
11.	Cisco	19	15	46	80
12.	Huawei	27	33	18	78
13.	Siemens	22	33	21	76
14.	IBM	23	12	39	74
15.	SAP	8	55	11	74



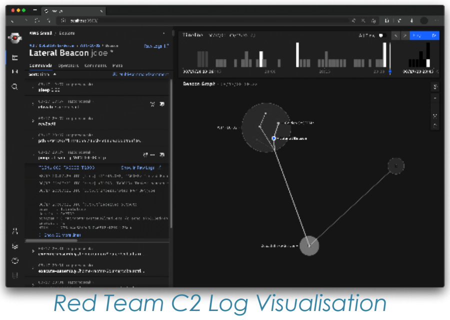
Count of vulnerabilities for top 15 vendors

Security App

CISA released Red Team Campaign Visualisation & Reporting Tool

Source: https://github.com/cisagov/RedEye, https://www.cisa.gov/

RedEye is an interactive open-source analytic tool designed and developed by Cybersecurity and Infrastructure Security Agency (CISA) to assist Red Teams with visualising and reporting command and control activities. This tool was released on GitHub in October 2022 and it allows an operator to assess and display complex data, evaluate mitigation strategies and enable effective decision making in response to a Red Team assessment. This tool parses logs such as those from Cobalt Strike and presents the data in an easily digestible format. Users can tag and add comments to the activities displayed within the tool. Operators can use RedEye's presentation mode to present findings and workflow to the stakeholders.

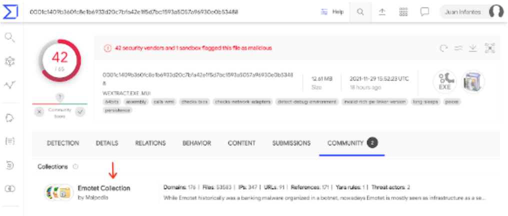


Red Team C2 Log Visualisation

Google Making Cobalt Strike Pentesting Tool harder to Abuse

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

Cobalt strike is a legitimate red teaming tool that consists of a collection of utilities in a JAR file that can emulate real cyber threats. It uses a client-server approach to provide the attacker with control over infected systems from a single interface. Google said that, "The stagers, templates and beacon are contained within the Cobalt strike JAR file and Cobalt strike provides basic protection using a reversible XOR encoding". Google focused on Cobalt strike versions by crafting hundreds of unique signatures that were integrated as a collection of community signatures available in VirusTotal. Google released these signatures as an open source to cybersecurity vendors.



0001c1409b360fc8e1b6933d20c7bfa42e1f5d7bc1593a5057a96930e0b53488

42 security vendors and 1 sandbox flagged this file as malicious

0001c1409b360fc8e1b6933d20c7bfa42e1f5d7bc1593a5057a96930e0b5348 8
WEXTRACT.EXE .MUI
64bits assembly calls-wmi checks-bios checks-network-adapters detect-debug-environment invalid-rich-pe-linker-version long-sleeps peexe persistence

12.61 MB
Size

2021-11-29 15:52:23 UTC
18 hours ago

Emotet Collection
by Malpedia

Domains: 176 | Files: 53583 | IPs: 347 | URLs: 91 | References: 171 | Yara rules: 1 | Threat actors: 2
While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a se...

VirusTotal IoC Collections

KataOS 'Verifiably Secure' OS for Embedded Devices

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

Google Open Source

Google initiated a project to focus on building a secure embedded platform for Machine Learning (ML) applications. This project goal is to design intelligent ambient ML systems that are secure and trustworthy. This project was named as Sparrow and it revolves around a new operating system named KataOS. Google said that, "KataOS provides a verifiably secure platform and it safeguards the user's privacy because it is logically non-viable for applications to breach the kernel's hardware security protections and system components are verifiably secure".

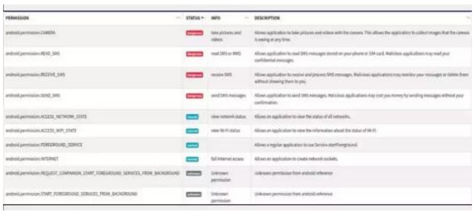
This project goal is to design intelligent ambient ML systems that are secure and trustworthy.

Mobile Security

Fake Reliance Jio Tower Malicious App Can Steal Financial Data

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

Cybersecurity firm Technisanct's researchers have discovered a Trojan JioTower.apk (Banking Trojan) which is capable of stealing personal and financial data. The JioTower.apk App is spreading via a phishing website https://rewardapps[.]xyz. This website is redirected to download a banking Trojan named Reliance Jio Tower. This app is a banking malware pretending as a legitimate Jio Tower mobile application. This malware is capable of stealing all personally identifiable information such as PAN number, Aadhar number, SMS messages, OTPs and bank information. This banking Trojan uses 10 risky permissions and steals user's information. Some risky permissions are like receive and send SMS, camera access, read contacts, device location and call logs. After installation app receives instructions from CCS (Command and Control Server). Instructions received from CCS not only take photos with the camera but also delete files, record calls and place calls. The app puts all notifications on silent mode to prevent getting noticed.



PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.REQUEST_COMPANION_START_FOREGROUND_SERVICES_FROM_BACKGROUND	unknown	Unknown permission	Unknown permission from android reference
android.permission.START_FOREGROUND_SERVICES_FROM_BACKGROUND	unknown	Unknown permission	Unknown permission from android reference

Critical permissions used by fake Jio Tower mobile application

The JioTower.apk App is spreading via a phishing website https://rewardapps[.]xyz. This website is redirected to download a banking Trojan named Reliance Jio Tower.

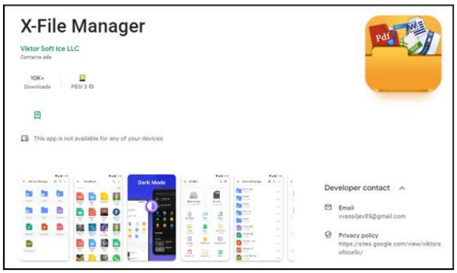
Android File Manager App Infects Devices with SharkBot Malware

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

Sharkboat is a dangerous banking trojan constantly evolving and posing as a file manager on the official Google Play Store by bypassing the app markets restrictions. Sharkboat malware is using following two android file manager apps and one cache cleaner app as a dropper:

- X-File Manager(com.victorsoftice.llc)-10k downloads
- FileVoyager(com.potsepko9.FileManagerApp)- 5k downloads
- LiteCleaner M (com.ltdevelopergroups.litecleaner.m) – 1k downloads

This malware steals banking information by displaying a fake login screen over legitimate login prompts in banking apps. The trojan's primary goal is to initiate ATS (Automatic Transfer Services) technique from compromised devices. The malware performs anti-root and anti-emulator checks and evades detection. As per Bitdefender notes, this malware has targeted a list of banking mobile apps as displayed. However, remotely threat actors can update this list anytime. As these apps are distributed from Google playstore, the best way to protect is to keep the play protect service enabled so that apps are uninstalled as they are detected as malicious. Antivirus applications would help to detect malicious apps and traffic.



X-File Manager

Viktor Soft Ice LLC

Contains ads

10K+ Downloads

PEGI 3

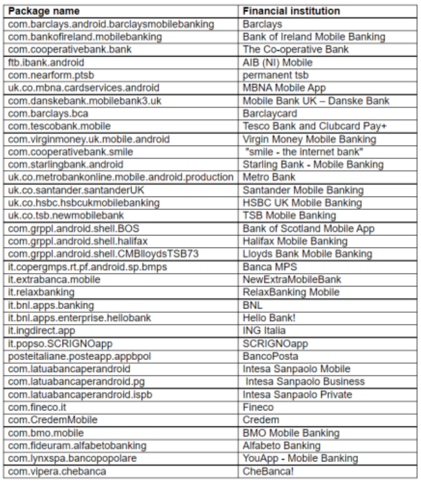
This app is not available for any of your devices

Developer contact

Email vvassiljev85@gmail.com

Privacy policy https://sites.google.com/view/viktors-officellc/

Malware X-File Manager on Google play (Source: Bitdefender)



Package name	Financial institution
com.barclays.android.barclaysmobilebanking	Barclays
com.bankofireland.mobilebanking	Bank of Ireland Mobile Banking
com.cooperativebank.bank	The Co-operative Bank
ftb.ibank.android	AIB (NI) Mobile
com.nearform.ptsb	permanent tsb
uk.co.mbna.cardservices.android	MBNA Mobile App
com.danskebank.mobilebank3.uk	Mobile Bank UK – Danske Bank
com.barclays.bca	Barclaycard
com.tescobank.mobile	Tesco Bank and Clubcard Pay+
com.virginmoney.uk.mobile.android	Virgin Money Mobile Banking
com.cooperativebank.smile	"smile - the internet bank"
com.starlingbank.android	Starling Bank - Mobile Banking
uk.co.metrobankonline.mobile.android.production	Metro Bank
uk.co.santander.santanderUK	Santander Mobile Banking
uk.co.hsbc.hsbcukmobilebanking	HSBC UK Mobile Banking
uk.co.tsb.newmobilebank	TSB Mobile Banking
com.grppl.android.shell.BOS	Bank of Scotland Mobile App
com.grppl.android.shell.halifax	Halifax Mobile Banking
com.grppl.android.shell.CMBlloydsTSB73	Lloyds Bank Mobile Banking
it.copergmps.rt.pf.android.sp.bmps	Banca MPS
it.extrabanca.mobile	NewExtraMobileBank
it.relaxbanking	RelaxBanking Mobile
it.bnl.apps.banking	BNL
it.bnl.apps.enterprise.hellobank	Hello Bank!
it.ingdirect.app	ING Italia
it.popso.SCRIGNOapp	SCRIGNOapp
posteitaliane.posteapp.appbpol	BancoPosta
com.latuabancaperandroid	Intesa Sanpaolo Mobile
com.latuabancaperandroid.pg	Intesa Sanpaolo Business
com.latuabancaperandroid.ispb	Intesa Sanpaolo Private
com.fineco.it	Fineco
com.CredemMobile	Credem
com.bmo.mobile	BMO Mobile Banking
com.fideuram.alfabetobanking	Alfabeto Banking
com.lynxspa.bancopopolare	YouApp - Mobile Banking
com.vipera.chebanca	CheBanca!

Banks targeted by this Sharkbot campaign (Source: Bitdefender)

Zanubis: Banking Trojan Targeting Banks and Social Media Apps

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

A Twitter post mentioning a new android banking trojan was found by Cyble Research. After an in-depth analysis, it has been found that this overlay-based banking trojan is targeting over 40 banking apps from Peru. The responses received from the C&C server located at hxxp://92.38.132[.]217:8000 by the Threat Actor (TA) are decrypted by using the string "Zanubis", hence the malware is referred to as "Zanubis". To pretend to be a legitimate application to the user, Zanubis appears as a PDF application and targets banks in Peru as well as social media apps like WhatsApp and Gmail. Out of 30 requested permissions, 10 permissions are exploited by the TA which includes Contacts, SMS, Camera, Audio, External Storage etc. After installation, this malware asks for Accessibility and Battery Optimisation permissions to automatically grants all the required permissions and connects to the C&C server to get the list of target applications along with the URLs of the overlay pages.

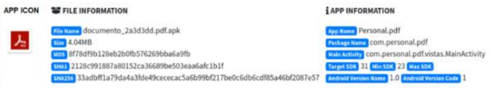
APK Metadata Info:

App Name: Personal.pdf

Package Name: com.personal.pdf

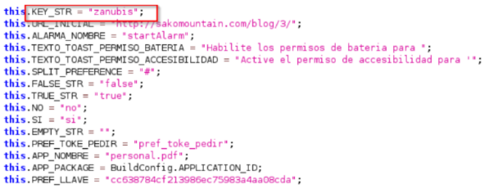
SHA256 Hash: 33adbff1a79da4a3fde49cececac5a6b99bf217be0c6db6cdf85a46bf2087e57

C&C Server: hxxp://92.38.132[.]217:8000



APP ICON	FILE INFORMATION	APP INFORMATION
	File Name documento_2a3d3dd.pdf.apk	App Name Personal.pdf
	Size 4.04MB	Package Name com.personal.pdf
	MD5 8f78df9b128eb2b0fb576269bba6a9fb	Main Activity com.personal.pdf.vistas.MainActivity
	SHA1 2128c991887a80152ca36689be503eaa6afc1b1f	Target SDK 31 Min SDK 23 Max SDK
	SHA256 33adbff1a79da4a3fde49cececac5a6b99bf217be0c6db6cdf85a46bf2087e57	Android Version Name 1.0 Android Version Code 1

Zanubis Metadata Information



```
this.KEY_STR = "zanubis";
this.URL_INICIAL = "http://sakomountain.com/blog/3/";
this.ALARMA_NOMBRE = "startAlarm";
this.TEXTO_TOAST_PERMISO_BATERIA = "Habilite los permisos de bateria para ";
this.TEXTO_TOAST_PERMISO_ACCESIBILIDAD = "Active el permiso de accesibilidad para '";
this.SPLIT_PREFERENCE = "#";
this.FALSE_STR = "false";
this.TRUE_STR = "true";
this.NO = "no";
this.SI = "si";
this.EMPTY_STR = "";
this.PREF_TOKE_PEDIR = "pref_toke_pedir";
this.APP_NOMBRE = "personal.pdf";
this.APP_PACKAGE = BuildConfig.APPLICATION_ID;
this.PREF_LLAVE = "cc638784cf213986ec75983a4aa08cda";
```

Decryption key used by TA

After installation, this malware asks for Accessibility and Battery Optimisation permissions to automatically grants all the required permissions and connects to the C&C server to get the list of target applications along with the URLs of the overlay pages.

Hard-Coded AWS Credentials in Android and iOS Apps Pose Risk

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

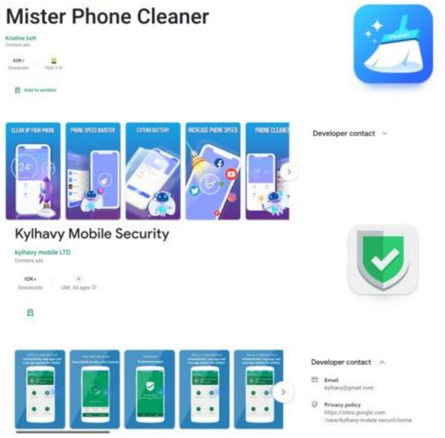
Generally, the hard-coded credentials are used by developers for authenticating to cloud services, accessing configuration files etc. Problem arises when the same access token is used for accessing all the files instead of a relevant one. By inserting an AWS hard-coded access key in a third-party SDK that gives access to its service, it exposes not only the private data of the app that uses the SDK but also the private data of all apps that use the same third-party component. Over 1,800 apps across Android and iOS have been identified by the researchers in Symantec Enterprise containing hard-coded Amazon Web Service (AWS) credentials. Almost 77% of the apps contains AWS access tokens allowing access to private data in AWS cloud. Although developed and maintained by other companies, almost half of the identified apps use the same AWS tokens. Five iOS banking apps have been identified using the same AI Digital Identity SDK, leaking fingerprint information for more than 3,00,000 users. Also, 16 different online gambling apps found exposing all AWS cloud services with root account credentials.

By inserting an AWS hard-coded access key in a third-party SDK that gives access to its service, it exposes not only the private data of the app that uses the SDK but also the private data of all apps that use the same third-party component.

SharkBot Malware Penetrates in Google Play Store Again

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

NCC Group shared a blog post about updated version of SharkBot is resurfacing on Google Playstore. It is a Trojan malware that steals user credentials and other data from bank apps. This malware was observed in 'Mister Phone Cleaner App and Kylhavy Mobile Security App and collectively installed 60,000 times. Both have been removed from the Google Playstore now. The malware was designed to target users in Spain, Poland, Germany, U.S., Austria, and Australia. According to Fox-IT Researchers the new dropper does not rely on android accessibility permissions for installation instead it asks users to install the malware as a fake update for antivirus to stay protected against threats. The Malware also removed Direct Reply feature which was used to reply directly to the notifications made on infected devices. In the latest update of SharkBot malware, it has now additional capabilities to steal the session cookies from the victims who have logged to their bank accounts.

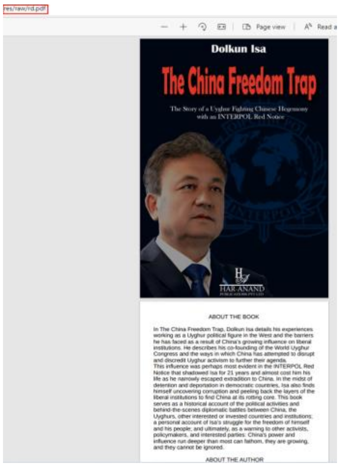


Play Store listings for two apps recently found to include the SharkBotDropper (source: Fox IT)

Android Spyware Campaign Targets the Uyghur Community

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

The security researchers from Cyble Research & Intelligence Labs (CRIL) have shared information about the Android malware targeting the Uyghur Community under the guise of the book 'The China Freedom Trap', a biography written by the exiled Uyghur leader Dolkun Isa. Upon analysis it was observed that the malware has an icon similar to the cover page of the book. On opening the app, malicious app leverages to steal device information, SMS, Contacts, Call logs, and neighbouring cell information etc. Also, the malicious app can capture the device screen and take pictures from the device's camera. The malware connects to the Threat Actor's server to and send data from the victim's device to the server.



ABOUT THE BOOK

In The China Freedom Trap, Dolkun Isa details his experiences working as a Uyghur political figure in the West and the barriers he has faced as a result of China's growing influence on liberal institutions. He describes his co-founding of the World Uyghur Congress and the ways in which China has attempted to disrupt and discredit Uyghur activism to further their agenda.
This influence was perhaps most evident in the INTERPOL Red Notice that shadowed Isa for 21 years and almost cost him his life as he narrowly escaped extradition to China. In the midst of detention and deportation in democratic countries, Isa also finds himself uncovering corruption and peeling back the layers of the liberal institutions to find China at its rotting core. This book serves as a historical account of the political activities and behind-the-scenes diplomatic battles between China, the Uyghurs, other interested or invested countries and institutions; a personal account of Isa's struggle for the freedom of himself and his people; and ultimately, as a warning to other activists, policymakers, and interested parties: China's power and influence run deeper than most can fathom, they are growing, and they cannot be ignored.

ABOUT THE AUTHOR

rd.pdf File

NCIIPC Initiatives

NCIIPC at C3ihub IIT Kanpur

Sh. Navin Kumar Singh, DG, NCIIPC visited Cybersecurity and Cybersecurity for Cyber-Physical Systems Innovation Hub (C3iHub), IIT Kanpur on 17th October 2022. He discussed Cyber Security Maturity Model and various other aspects of Cyber Security with the IIT Kanpur dignitaries. The other members participated in the discussion were Prof. Sandeep Shukla (Joint Director of C3iHub IIT Kanpur), Prof. Manindra Agrawal (Deputy Director of IIT Kanpur), Sh. Ranjeet Mishra (Chief Business Officer, C3iHub IIT Kanpur), and Ms. Tanima Hajra (Chief Operating Officer, C3iHub IIT Kanpur).

DG NCIIPC with the IIT Kanpur dignitaries

POSOCO CISO Meet

A CISO meet for power sector utilities was organised by Power System Operation Corporation Limited (POSOCO) on 9th November 2022 for southern region Power Sector utilities. The meeting discussed on how to implement the guidelines for cyber security in power sector and the challenges for same. The meeting was attended by Director South, NCIIPC who also suggested importance of various cyber security controls in Power Sector.

NCIIPC Celebrated Cyber Security Awareness Month

NCIIPC conducted Cyber Security Awareness Event for Power Sector entities on 11th October 2022. The event was attended by more than 300 participants.

NCIIPC conducted Cyber Security Awareness Quiz for critical sector organisations during 21-31 October 2022. Total 197 organisations and 12425 employees participated in this quiz.

#NCSAM2022
Capacity Building is Crucial
National Critical Information Infrastructure Protection Centre
NCIIPC
A unit of NTRO
nciipc.gov.in
@NCIIPC

NCIIPC conducted Cyber Security Awareness Event for Power Sector Entities on 11 October 2022.
The event was attended by more than 300 participants.

Webinar on Cyber Security Awareness Program for Public, Private Banks and Regional Rural Banks (RRBs) was held on 19th October 2022 by NCIIPC. Around 119 officials from various banks attended this webinar.

A webinar on "Cyber Security Awareness Program for Transport Sector Entities" was organised by NCIIPC on 18 Oct 2022. Approximately 135 participants from various transport sector organisations across the country participated in the online webinar program. The first session of the webinar was on Indian Railway, Metro Rails and Ministry of Road Transport and Highways (MoRTH), and the second half of the webinar was on Aviation and Shipping.

A webinar on "Cyber Security Awareness Program for Government Sector Entities" was organised by NCIIPC on 12 Oct 2022. Various government sector organisations across the country participated in the online webinar program.

A cyber security awareness program for Strategic & Public Enterprises (S&PE) sector organisations was conducted on 27th Oct 2022. A total of 53 participants from S&PE organisations: Indian Space Research Organisation (ISRO), Department of Atomic Energy (DAE), Ministry of Earth Sciences (MoES) and Bharat Heavy Electricals Limited (BHEL) attended the program.

A cyber security awareness program for Health sector organisations was conducted on 28th Oct 2022. Total 32 participants from Health sector (National Health Authority (NHA), Ministry of Health & Family Welfare (MoHFW), Department of Biotechnology, Ministry of Ayush and Indian Council of Medical Research (ICMR)) attended the program.

NCIIPC West Zone organised 'Cyber Security Awareness Program for Security Markets' webinar for banking industry during Cyber Security Awareness Month on 20th October 2022.

A webinar on 'Cyber Security Awareness Program for Telecom Sector Entities' was organised by NCIIPC on 27th October 2022. Around 100 participants from various telecom sector organisations across the country participated in the online webinar program.

DG NCIIPC with other dignitaries at Cyber Security Symposium

NCIIPC at POSOCO Cyber Security Symposium

POSOCO organised a Cyber Security Symposium for CERT-GRID on the occasion of Cyber Jagruk Diwas on 2nd Nov 2022 at New Delhi. Sh. Navin Kumar Singh, DG NCIIPC and other senior dignitaries, stakeholders and cyber security experts from SLDCs, Industries, Statutory Bodies, and Academic participated in the symposium.

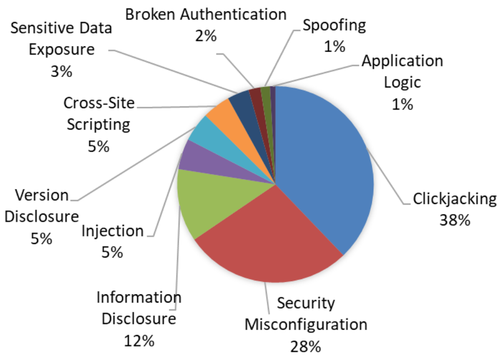
NCIIPC Responsible Vulnerability Disclosure Program

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 2783 vulnerabilities reported during the last quarter of 2022. The top 10 vulnerabilities are:

- Clickjacking
- Security Misconfiguration
- Information Disclosure
- Injection

- Version Disclosure
- Cross-Site Scripting
- Sensitive Data Exposure
- Broken Authentication
- Spoofing
- Application Logic



Around 358 researchers participated in RVDP programme during the last quarter of 2022. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Abhiney Sharma
- Alimurtuza A Patrawala
- Amal Vijay
- Arul NV
- Dileesh D.
- Dinesh Kumar
- Dinesh N
- Jayesh Thakur
- Madhurendra Kumar
- Meet Narkhede
- No Name (Name of researcher is not available)
- Prince S
- Shobit Vangule
- Vedant Roy
- Vijay Sutar

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				

FEBRUARY 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				

Upcoming Events - Global

January 2023

• FloCon 2023, Santa Fe	9-12 Jan
• Convene: Security Training and Awareness Conference, Clearwater	10-11 Jan
• Health-ISAC Healthcare Cybersecurity Workshop, Prague	12 Jan
• SANS Security East 2023, New Orleans & Virtual	16-21 Jan
• CactusCon 2023, Arizona	27-28 Jan
• Data Connectors Cybersecurity Conference Columbus, Columbus	19 Jan
• The Cybersecurity Meetup 2023, Toronto	31 Jan

February 2023

• Stop Zero-Day Malware with Zero Stress Europe, Virtual	1 Feb
• What's Brewing In Cloud Security, Virtual	2 Feb
• FutureCon Chicago CyberSecurity Conference, Chicago & Virtual	8 Feb
• IT-DEFENSE 2023, Mainz	8-10 Feb
• 4th CISO 360 Middle East, Dubai	9-10 Feb
• HACKRON 2023, Tenerife	17 Feb
• Hackplayers Conference (Hc0n), Madrid	24-25 Feb
• Blockchain Economy London Summit, London	27-18 Feb

March 2023

• SnowFROC 2023, Denver	2 Mar
• Blockchain Economy Dubai Summit, Dubai	8-9 Mar
• FutureCon Detroit Cybersecurity Conference, Detroit & Virtual	9 Mar
• NULLCON Berlin, Berlin	9-10 Mar
• APIsecure, Santa Clara	14-15 Mar
• Nigeria Cybersecurity Summit 2023, Lagos	16-17 Mar
• International Conference and Expo on Cyber Security and Networking, Virtual	20-21 Mar
• Kansas City Cybersecurity Conference, Kansas City	30 Mar

April 2023

SnowFROC 2023, Denver	2 Mar
ItaliaSec: IT Security Conference, Rome	4-5 Apr
FutureCon Virtual Central Conference, Virtual	5 Apr
Botconf 2023, Strasbourg	11-14 Apr
Cybersecurity for Critical Assets Singapore, Singapore	18-19 Apr
Cyber Security EXPO, Bristol	20 Apr
Bsides NYC 2023, New York	22 Apr
RSA Conference 2023, San Francisco	24-27 Apr
NZ Government Data Summit, Wellington	26-28 Apr

Upcoming Events - India

SANS Secure India 2023, Bengaluru & Virtual	13-25 Mar
30th Convergence India expo, New Delhi	27-19 Mar
Cybersecurity Summit: Bengaluru, Bengaluru & Virtual	12-13 Apr
Global Legal ConfEx, New Delhi	19 Apr

Convergence India Expo | 27-29 MARCH 2023
Pragati Maidan, New Delhi

ItaliaSec
SECURING ITALY FROM
CYBER THREATS

#CS4CA
CYBER SECURITY FOR CRITICAL ASSETS
APAC

MARCH 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	

APRIL 2023

S	M	T	W	T	F	S
30						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

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

- AD DS: Active Directory Domain Services
- AP: Associated Press
- APT: Advanced Persistent Threat
- ATS: Automatic Transfer Services
- AWS: Amazon Web Service
- BHEL: Bharat Heavy Electricals Limited
- C&C/C2: Command & Control
- CCS: Command and Control Server
- CDSL: Central Depository Services (India) Limited
- CEA: Central Electricity Authority
- CII: Critical Information Infrastructure
- CISA: Cybersecurity and Infrastructure Security Agency
- CMMS: Census Monitoring & Management System
- CRS: Civil Registration System
- CVE: Common Vulnerabilities and Exposures
- DAE: Department of Atomic Energy
- DC: Data Centre
- DDOS: Distributed Denial of Service
- DIB: Defence Industrial Base
- DLL: Dynamic Link Library
- DOT: Department of Telecommunications
- DRS: Disaster Recovery Site
- EOL: End of Life
- FCC: Federal Communications Commission
- FTP: File Transfer Protocol
- HL: House Listing
- HTTP: Hypertext Transfer Protocol
- HVCI: Hypervisor-protected Code Integrity
- IIS: Internet Information Services
- ISRO: Indian Space Research Organisation
- MEITY: Ministry of Electronics and Information technology
- MHA: Ministry of Home Affairs
- ML: Machine Learning
- MLV II: Memory Loader Verifier II
- MoES: Ministry of Earth Sciences
- MoHFW: Ministry of Health & Family Welfare
- MoRTH: Ministry of Road Transport and Highways
- MSP: Managed Service Provider
- MSSQL: Microsoft SQL
- NCIIPC: National Critical Information Infrastructure Protection Centre
- NDC: National Data Centre
- NHA: National Health Authority
- NIC: National Informatics Centre
- NLDC: National Critical Information Infrastructure Protection Centre
- NOTAM: Notice to Air Mission

- NPR: National Population Register
- NSA: National Security Agency
- NSCS: National Security Council
- NVD: National Vulnerability Database
- ORGI: Office of the Registrar General of India
- PE: Population Enumeration
- PKS: Process Knowledge System
- POSOCO: Power System Operation Corporation Limited
- PS: Protected System
- QA: Quality Assurance
- RAS: Remote Access Server
- RAT: Remote Access Trojan
- RCC: Remote Compact Controller
- RDP: Remote Desktop Protocol
- RRB: Regional Rural Bank
- S&PE: Strategic & Public Enterprises
- SBOM: Software Bill of Materials
- SE: Self-Enumeration
- SLDC: Software Development Lifecycle
- TA: Threat Actor
- TPM: Trusted Platform Module
- TTP: Tactic, Technique and Procedure

Notes

National Critical Information Infrastructure Protection Centre

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.