



NEWSLETTER

July 2021



National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)



Beware of Ransomware

Epsilon Red fivehands Sekhmet cerber SYNack Sarbloh clop
tycoon cryptolocker wannacry darkside
agelocker revil nemty
Nephilim LockBit cryptowall bad rabbit
Usagoo Avaddon lockbit DoppelPaymer locky
netwalker maze greed ryuk goldeneye
jigsaw



Combatting Ransomware Attacks



Take Regular Data Backup



Implement Network Segmentation



Increase Cyber Security Awareness



Define Business Continuity Plan



Define Incident Response Plan



Apply Regular Security Updates



Install Antivirus



<https://nciipc.gov.in/>



@NCIIPC



NCIIPC India



NCIIPC India



helpdesk1@nciipc.gov.in



NCIIPC Newsletter

July 2021



Inside This Issue

- 1 **Message from NCIIPC Desk**
- 2 **News Snippets - National**
- 4 **News Snippets - International**
- 7 **Trends**
- 13 **Malware Bytes**
- 25 **Learning**
- 37 **Vulnerability Watch**
- 41 **Security App**
- 44 **Mobile Security**
- 46 **NCIIPC Initiatives**
- 48 **Upcoming Events – Global**
- 49 **Upcoming Events – India**

Message from the NCIIPC Desk

Dear Readers,

NCIIPC takes great pleasure in sharing with its Readers, the fact that India has been ranked 10th in the Global Cybersecurity Index (GCI) 2020. The rankings were released on 29 Jun 2021 by the United Nation's International Telecommunications Union (ITU) Global Cybersecurity Agenda (GCA), and are based on Legal, Technical, Capacity Building and Organisational measures. India, which was earlier ranked 47th, joins the US, the UK, France, Singapore and Russia in the Top 10, way ahead of China ranked at No 33 and Pakistan at No 79.

Another major development is that the Department of Telecommunications (DoT) has amended the licensing conditions for Telecom Companies to include Defence and National Security as essential parameters. It would be mandatory for Telecom Operators to procure equipment only from 'Trusted Sources' based on the list published by the Government. The operators will not only have to submit all the details regarding their Networks (core equipment, access equipment, transport equipment and support systems), the Telecom Operators and vendors will also have to provide a certificate that the equipment does not have any malware/backdoors and is free of all known vulnerabilities.

The cyberattack on the Colonial Pipeline on 7th May 2021, the largest pipeline system for refined oil products in the US, resulted in disruption of operations for five days, which caused a temporary fuel shortage along the East Coast. The event highlights the enormity of Ransomware threat to our Critical Information Infrastructure and the inescapable need, globally, for countries to collaborate with each other to ensure safety of National Critical Functions.

NCIIPC has been engaging with various professionals and security researchers to discover vulnerabilities in Critical Sector Organisations. During the last quarter, around 3000 vulnerabilities were reported by more than 300 security researchers. Their contribution towards strengthening the national cyber space is commendable.

NCIIPC immensely values the comments and suggestions from the readers. Based on the overwhelming response, the Newsletter Team is working towards publishing it monthly instead of quarterly with effect August 2021 issue.

Your feedback is solicited. Selected letters shall also be published. You may write to us at newsletter@nciipc.gov.in.

News Snippets - National

Ransomware Attack on MIDC Servers

Source: <https://mumbaimirror.indiatimes.com>, www.hindustantimes.com

Maharashtra Industrial Development Corporation's (MIDC) information technology applications went down on 21st March due to a Ransomware attack called "SYNack". This attack impacted the MIDC database servers. It impacted all applications and database servers that were hosted on Cloud DC and DR of Exuberant Support for Data Services (ESDS) and also local servers hosted at MIDC HQ in Mumbai. The ransomware encrypted the data that was stored on these servers. After the attack was discovered, all computers were disconnected from the server. MIDC asked all its departments to shut the systems until the issue was resolved completely. This shutdown caused disruption of services across the state. The corporation claimed that the backup files of its website were safe as those were stored in different networks. The restoration process was initiated from the same day, and customer facing portals such as MIDC website, Single-Window Clearance (SWC), Enterprise Resource Planning, and water billing system were made live after applying due security checks.



It impacted all applications and database servers that were hosted on Cloud DC and DR of Exuberant Support for Data Services (ESDS) and also local servers hosted at MIDC HQ in Mumbai.

Upstox suffers Data Breach, Leaks Millions of Users' Data

Source: <https://thehackernews.com/>

Online trading and discount brokerage platform Upstox suffered a security breach of its systems that resulted in exposure of sensitive information of approximately 2.5 million users on the dark web. The information leaked includes names, date of birth, email addresses, bank account details, and about 56 million KYC documents that were pulled from the company's server. The breach was disclosed by an independent researcher, on April 11. Upstox upgraded its security systems after this breach.



CERT-In Advisory on Facebook Data Leak

Source: <https://www.cert-in.org.in/>

The Computer Emergency Response Team (CERT-In) issued a public advisory (CIAD-2021-0017) for Indian Facebook users to secure their account information. The development came after the widely reported Facebook data breach that leaked information of 450 million Facebook users worldwide. The exposed information includes email ID, profile ID, Full name, occupation, birth date, and phone numbers. According to Facebook, the scraped information does not include any health information, financial information or passwords. The threat actors scraped the data prior to September 2019, using the



Cert-In added, Facebook also recommended account holders to enable the two-factor authentication.

"contact Importer" feature of Facebook. Facebook recommended the users to change their profile settings to "friends" or "private". Facebook also recommended account holders to enable the two-factor authentication.

Ransomware Supporting Farmers

Source: <https://cio.economictimes.indiatimes.com>, <https://cert-in.org.in/>



Image source:
<https://blogs.quickheal.com/>

In order to support protesting farmers in India, Threat actors have launched a new technique of ransomware attack that does not evoke money but conveying a message that no data will be recovered until the demands of the protesting farmers are met. The hacker group titled 'Khalsa Cyber Fauj' reported to be leading this attack in the country has targeted entities connected with farmers' protests. It has been discovered that the ransomware named as "Sarbloh", is being distributed through malicious word documents via emails, containing a political message supporting the farmers. This hacker group used military-grade encryption on system files to turn them useless.



According to SITA, the vendor serves around 90% of the world's airlines, which aggregates to 2,800 customers including airports, airlines, and government agencies.

4.5 million Air India Passengers' Data Stolen in SITA Cyberattack

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

Three months after global aviation industry IT supplier SITA fell victim to a cyber-attack, Air India revealed that the incident caused stealing of around 4.5 million of its passengers' data. The breach convoluted personal data spanning almost 10 years, from 26 August 2011 to 3 February 2021. The stolen information included name, contact information, passport information, date of birth, ticket information, Star Alliance, Air India frequent flyer data, and credit card data. No regular flyer passwords or CVV/CVC data were stolen, as this data was not held by SITA. SITA, an information technology and communications corporation is the data processor of Air India's passenger service system. Air India has been conducting investigations, engaging external specialists, securing compromised servers, notifying and liaising with credit card issuers, and resetting passwords of the Air India frequent flyer program. According to SITA, the vendor serves around 90% of the world's airlines, which aggregates to 2,800 customers including airports, airlines, and government agencies.

Loophole by which SMSes could be sent from Government IDs

Source: <https://gadgets.ndtv.com/>

In public shared usernames and passwords for the government's SMS publishing platform meant that a malicious manipulator could have used them to send text messages posing as the

government. Sai Krishna Kothapalli, a security researcher explained while searching through the public repositories on GitHub as a part of his research, he came across credentials which looked suspicious, because the project belonged to an Indian, and its URL is of government service. The service has been used by the government to send over 600 crore text messages every year. He also found an API for the service, which required 3 parameters to use - the username, password, and sender ID. Sender ID is the header that conveys where a message has come from, such as VX-ViCARE, or TX-MYTSKY for example or something that sounds very official, such as ADHPGOVT. Using this, the Researcher was able to test the API, and send messages to himself, posing as the Election Commission and the Himachal Government. This particular security flaw has been fixed by now.

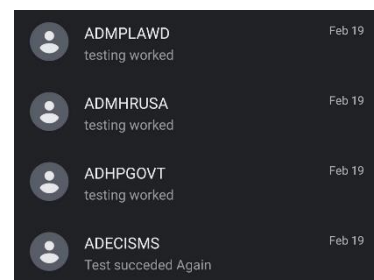


Image source:

<https://i.gadgets360cdn.com/>

News Snippets - International

Iran Nuclear Facility suffers Cyber-Attack

Source: <https://www.infosecurity-magazine.com>, <https://www.bbc.com>

A nuclear facility in Iran was hit by cyber-attackers. This cyber-attack caused a power failure at the Natanz complex nuclear facility. A day before the breach Iran's President Mr. Hassan Rouhani inaugurated new centrifuges at the Natanz site. Spokesperson for the Atomic Energy Organisation of Iran (AEOI) said that incident occurred in the morning of April 11 involving the nuclear facility's power network.



Natanz located at 250km south of the Iranian capital Tehran

FBI removed Backdoors from Vulnerable Servers

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

A court order allowed the Federal Bureau of Investigation (FBI) to enter networks of businesses to remove web shells used by cyber attackers exploiting the Microsoft Exchange vulnerabilities. The FBI removed malicious web shells from hundreds of computers in the United States that were running vulnerable versions of Microsoft Exchange Server. Hundreds of unmitigated web shells were identified and removed from hundreds of systems. This action of FBI helped keep many organisations secure but it also raised questions about the direction of cybersecurity. FBI acted on its own accord; it accessed the systems without knowledge of the organisations from which web shells were removed.



APT Hackers Breached US Local Govt. by Exploiting Fortinet Flaws

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

The Federal Bureau of Investigation (FBI) said that state-sponsored APT hackers breached the webserver of a U.S. municipal



Image source:

<https://1.bp.blogspot.com/>

government after hacking a Fortinet appliance. After gaining access to the local government organisation's server, the APT actors moved laterally through the network and created new domain controller, server, and workstation user accounts imitating already existing ones. FBI also detected attackers associated with this ongoing APT malicious activity creating 'WADGUtilityAccount' and 'elie' accounts on compromised systems. According to FBI, this APT group may use this access to gather and exfiltrate data from the victims' network. APT actors factually exploited critical vulnerabilities to conduct Distributed Denial-of-Service (DDoS) attacks, injection attacks, ransomware attacks, spear-phishing campaigns, website defacements, and disinformation campaigns. State-sponsored hackers have continuously aimed at unpatched Fortinet servers.



Attackers stole documents that contained more than 76,000 email addresses for employees and contractors for the Ministry of Land, Infrastructure, Transport, and Tourism

Hackers Stole Files from Government Agencies of Japan

Source: <https://threatpost.com/fujitsu-saas-hack-japan-scrambling/166517/>

Hackers have stolen files from several official government agencies of Japan by hacking into Fujitsu's Software-as-a-Service (SaaS) platform and gaining access to its systems. The Japan-based tech giant temporarily inactivated ProjectWEB enterprise after learning of the attack, which is known to have affected the Ministry of Land, Transport, and Tourism. ProjectWEB is a cloud-based enterprise collaboration and file-sharing platform since the mid-2000s, and which a number of agencies within the Japanese government currently use. Fujitsu decided to suspend the operation of ProjectWEB following pressure from NISC, Fujitsu's Cabinet Cyber Security Centre, making an apology "for the great concern and inconvenience" the breach caused its clients. The company said, "We will continue to work on inspecting and analysing the scope of impact and the causes of all projects that use [ProjectWEB] with the cooperation of our customers". The Japanese press claimed that attackers stole documents that contained more than 76,000 email addresses for employees and contractors for the Ministry of Land, Infrastructure, Transport, and Tourism. Data on air traffic control also was stolen from the Narita Airport, which serves Tokyo, according to a separate report by Japanese public broadcaster NHK.

Major U.S. Pipeline Crippled in Ransomware Attack

Source: <https://threatpost.com, www.bloomberg.com>

A ransomware attack ceased pipeline activities for the Colonial Pipeline Co., which delivers the East Coast with roughly 45 percent of its liquid fuels. Colonial Pipeline temporarily stopped pipeline operations in response to a cyberattack. On May 7, the Colonial Pipeline Company learned it was the victim of a

cybersecurity attack and as a safeguard, the company took key systems offline to avoid further infections. In response, the company proactively took certain systems offline to contain the threat, which has temporarily frozen all pipeline operations and affected some of their IT systems. Colonial Pipeline also dispensed an updated statement clarifying that they are working with the US Department of Energy to gradually bring segments of the pipeline back online. The FBI confirmed that the Russia-based hacker group DarkSide was behind the attack on Colonial Pipeline. The Colonial Pipeline paid \$4.4 Million (75 bitcoins) in ransom to the hacker group to recover its stolen data. Later, FBI seized 63.7 bitcoins that valued approximately \$2.3 million. The FBI was able to find the Bitcoin by uncovering the digital addresses used by the hackers to transfer the funds. The Colonial Pipeline operations were restored on May 13, 2021.

The FBI was able to find the Bitcoin by uncovering the digital addresses used by the hackers to transfer the funds. The Colonial Pipeline operations were restored on May 13, 2021.

Ransomware Disrupted Tulsa's Online Services

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

The city of Tulsa, Oklahoma, suffered a ransomware attack that enforced the city to close up its systems to avert the further spread of the malware. Threat actors deployed a ransomware attack on the town of Tulsa's network that led to the city shutting down all of its systems and disturbing online services. The corporate stated that after they identified malware on their servers and instantly in an abundance of caution, they shut all of their systems down. However, the shutdown of City systems is stopping residents from accessing online bill payment systems, utility billing, and services through email. The websites for the town of Tulsa, Tulsa Police, the Tulsa City Council, and the Tulsa 311 websites also got down. In a Facebook post, the city told that customer information was compromised.

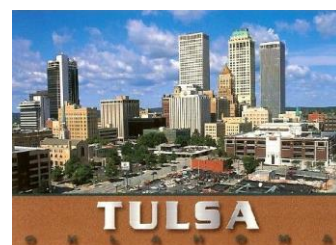


Image source: <https://i.pinimg.com/>

The websites for the town of Tulsa, Tulsa Police, the Tulsa City Council, and the Tulsa 311 websites are also down for maintenance.

Health Services around the World Targeted by Malwares

Source: [bleepingcomputer.com](https://www.bleepingcomputer.com), [securityweek.com](https://www.securityweek.com), [theregister.com](https://www.theregister.com)

Health services around the globe have been targeted by malware attack. New Zealand's Waikato District Health Board (DHB) was attacked with a strain of ransomware that shut down most IT services and drastically disrupted services at six of its affiliate hospitals. The attack inactivated all IT services except email. Patient notes became inaccessible, clinical services were interrupted, and surgeries postponed. Phone lines went down and hospitals were forced to admit urgent patients only. The Alaska health department in a statement said its website was the target of a malware attack and was taken offline. Ireland's Health Service Executive (HSE) also shut down all of its IT systems on 14 May after suffering a Conti ransomware attack. The IT systems were taken



Image source: <https://media-exp1.licdn.com/>

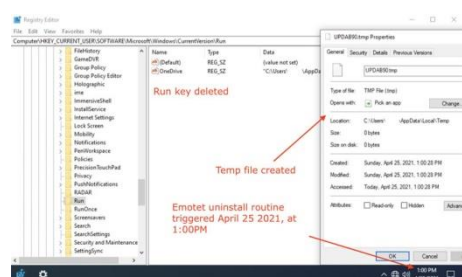
Ireland's Health Service Executive (HSE) also shut down all of its IT systems on 14 May after suffering a Conti ransomware attack.

offline in order to protect the systems from attack and to allow HSE to fully assess the situation with its security partners. This IT outage led to widespread disruption in the country's healthcare, causing limited access to medical records and diagnostics, there were transcription errors due to handwritten notes, and faced slow response times to healthcare visits.

Trends

Software Update Deleting Botnet from Infected PCs

Source: <https://www.zdnet.com>, <https://blog.malwarebytes.com>



Emotet-infected machine triggered its uninstallation routine

A special update was created by law enforcement in U.S., Canada and Europe in order to conduct a coordinated takedown of Emotet infrastructure. This law enforcement triggered the process of uninstalling Emotet, the world's largest botnet, from 1.6 million infected computers around the world. The law enforcement officials delivered an Emotet update, "EmotetLoader.dll" file, which removed the malware from all infected devices. The updated bot contained a clean-up routine responsible for uninstalling Emotet after the April 25 2021 deadline. The Windows registry run key of infected devices is removed to make certain that the Emotet modules will not start automatically and all servers running Emotet processes are terminated. This switch-off process does not remove other installed malware on infected devices via Emotet, nor any malware from other sources.

Microsoft uses ML to Predict Attackers' Next Steps

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



Image source: <https://internetofbusiness.com/>

This threat intelligence and machine learning model uses TTPs from attack chain, MITRE ATT&CK framework, and the massive dataset of trillions of daily security signals from its 400,000 customers to model threat actors.

Microsoft researchers are developing ways to use machine learning (ML) to turn attackers' specific approaches to compromising targeted systems into models of behaviour that can be used to automate the attribution of attacks to specific actors and predict the most likely next attack steps. The researchers are using the collected data on threat actors by its cloud security and endpoint products to train a probabilistic machine-learning model that is capable of associating a series of Tactics, Techniques and Procedures (TTPs) with a specific group. The model can also predict the next attack step that defenders will observe. This threat intelligence and machine learning model uses TTPs from attack chain, MITRE ATT&CK framework, and the massive dataset of trillions of daily security signals from its 400,000 customers to model threat actors. The TTPs will be used as variables in a Bayesian network model to correlate alerts from various detection systems and predict the future attack stages. This model can easily be updated with new information when attackers change their approaches in compromising the target.

Cybersecurity in European Railways

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

The ENISA-ERA (ENISA, the EU Agency for Cybersecurity, and ERA-the EU Agency for Railways) Conference: "Cybersecurity in Railways" introduced the latest cybersecurity developments and highlighted the main challenges in this field. Cybersecurity is a key requirement to enable railways to deploy and take advantage of the full extent of a digital and connected environment. The European Commission proposed the revision for Network Information Security Directive (NIS2) to strengthen the cybersecurity measures that are adopted by the Member States and used by European Railway Undertakings (RU) and Infrastructure Managers (IM). A cybersecurity toolkit has been developed and shared with the participants. Shift2Rail and the Technical Demonstrator 2.11, a smart radio-connected all-in-all wayside objects, would demonstrate the applicability of their findings on specific projects such as Automatic Train Operation or Adaptable Communication Systems. Shift2Rail is also developing a proposal for European Computer Security Incident Response Team, called 4SECURERAIL project, for identified threats to be instantly shared with targeted railway stakeholders.



Cybersecurity is a key requirement to enable railways to deploy and take advantage of the full extent of a connected, digital environment.

Japan to Restrict Private Sector Use of Foreign Equipment & Tech

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

The Japanese government will allegedly introduce new guidelines across 44 sectors to bolster national cyber defence, partly in response to the Colonial Pipeline hack that occurred recently. The government plans to improve various laws governing each sector through passing an all-encompassing motion and a new law demanding each sector to be sensible of national security risks. The sectors that are anticipated to see the legislative changes include telecommunications, electricity, finance, railroads, government services, and healthcare, among others. Specifically, these sectors will apparently be required to look into issues stemming from the use of foreign equipment or services, including cloud data storage and connections to servers positioned overseas. The government will also supposedly monitor companies for compliance and gain the power to prevent companies from using foreign equipment if they notice any major issues. Detailed standards will likely be defined in future government ordinances and guidelines as well. Other countries, like the US, have already enforced similar restrictions on tech-related procurement.

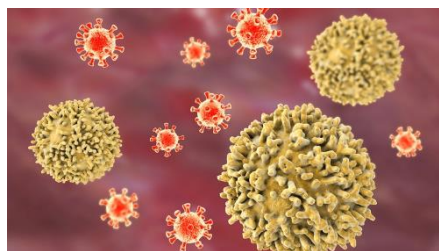


JAPAN GOV
THE GOVERNMENT OF JAPAN

The sectors that are anticipated to see the legislative changes include telecommunications, electricity, finance, railroads, government services, and healthcare, among others.

Self-healing Cybersecurity Software

Source: <https://pcsi.nl/>



The renewal process ensures that there are more moments at which cyberattacks can be intercepted.

An additional functionality of this software is to renew the containers at adjustable intervals.

A 'self-healing' cybersecurity software was developed by ABN AMRO (Algemene Bank Nederland-Amsterdam Rotterdam Bank) and TNO (The Netherlands Organisation for applied scientific research). This software has capability to autonomously adapt to factors that could disrupt the computer systems. It is based on the way human cells fight against bacteria and viruses and then renew themselves. This idea has been translated into a concept for ICT (Information and Communications Technology) security. The renewal technique is based on the existing ICT technology: Kubernetes. An additional functionality of this software is to renew the containers at adjustable intervals. The renewal process ensures that there are more moments at which cyberattacks can be intercepted. This software includes anomaly detection so that any containers with unusual behaviour are immediately terminated without having to pass through a central system. This allows much faster and more local intervention if something goes wrong. This is based on human immune system that uses a replacement principle or 'disposability' process to kill cells it suspects are infected, and replace them by 'clean' cells. This biological property fits well with today's cybersecurity problems. In cybersecurity the main problem is reactivity. A cyberattack generally cannot be detected or predicted in time, so organisations are always one step late to respond. The damage has already been done. In order to anticipate this, the self-healing security software seems promising.

Energy Sector Witnesses a Rise in Cyberattacks

Source: <https://cyware.com/>



Most of the attacks have been perceived in North America, followed by Europe and Asia. Hafnium, the notorious hacker group, engaged in several attacks and battered over 200 Bangladeshi organisations.

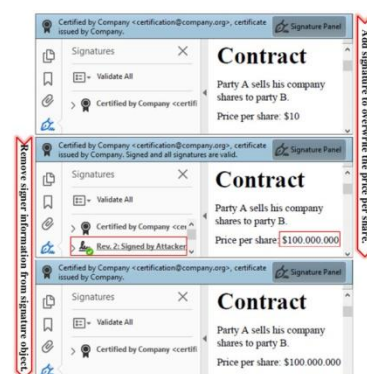
The growing adoption of new technology in the energy sector is leading to an upsurge in cyberattacks and related risks, as well. In recent days, there have been several cyberattacks targeted at the energy and power sector. Most of the attacks have been perceived in North America, followed by Europe and Asia. Hafnium, hacker group, engaged in several attacks and battered over 200 Bangladeshi organisations. In this operation, the group targeted several industries, including energy and power. Bourbon Corporation, a global leader in marine services for offshore oil and gas, was hit by a cyberattack that blocked its computer system. Shell Oil Co. and RaceTrac Petroleum Inc. were impacted by a cybersecurity incident as a result of the Accellion FTA hack. Royal Dutch Shell, the multinational oil and Gas Company, was compromised by Clop ransomware. Threat actors siphoned off sensitive documents and then disclosed workers' passports and visa scans to compel for a quick ransom payment. REvil ransomware attacked Standley Systems and claimed to acquire

service contracts, medical documents, personal data, and more in the attack. The energy sector functions critical infrastructure and disruptions at such facilities could lead to overwhelming outcomes. Therefore, organisations operating in the sector are recommended to deploy suitable security measures to stay protected from growing cyberattacks.

Certified PDF Documents Hacked using EAA and SSA

Source: <https://thehackernews.com/>

Cybersecurity researchers have found two new attack techniques on certified PDF documents that could enable attacker to modify document's visible content by malicious content without invalidating its signature. Two attacks dubbed as Evil Annotation Attack (EAA) and Sneaky Signature Attack (SSA) manipulates the PDF certification process by exploiting flaws in implementation of digital signatures. Certification signature allows different subsets of modifications on the PDF document according to permission level set by the certifier. In Evil Annotation Attack (EAA) attackers modify certified document that's provisioned to insert annotations by including annotation containing malicious code. In PDF documents signer can insert signature field at exact position, can define appearance and content. Each new signature contains new signer's information. Attacker can misuse this feature of PDF document to stealthily manipulate the document. In Sneaky Signature attack (SSA) manipulates the appearance by adding overlaying signature elements to document that allows filling out form fields. 15 of 26 PDF applications including adobe acrobat reader (CVE-2021-28545 and CVE-2021-28546) (CVE-2020-35931), Foxit Reader and Nitro Pro are found vulnerable to the EAA attack. These vulnerabilities allow attackers to execute high-privileged JavaScript code redirects user to malicious website. To mitigate such kind of attacks researchers, recommend to prohibit the use of FreeText, Stamp and Redact annotations. Researchers created a python-based utility called PDF-detector which parses certified documents to found suspicious element in the PDF document.

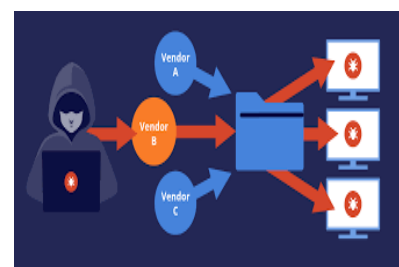


Two attacks dubbed as Evil Annotation Attack (EAA) and Sneaky Signature Attack (SSA) manipulates the PDF certification process by exploiting flaws in implementation of digital signatures.

Recent Trends in Supply Chain Attack

Threat Assessment Team, NCIIPC

A supply chain attack also called Third Party attack or value chain is a cyber-attack strategy in which an attacker infiltrates through outside vendors and get access of sensitive data of an organisation by exploiting vulnerabilities in its supply chain mechanism. It continues to be feature of threat landscape, with an increase by 78% in last year. Attack takes place on less secure elements in supply chain. A data infiltration through a third-party vendor is possible because vendors require access to sensitive



A data infiltration through a third-party vendor is possible because vendors require access to sensitive data to integrate and configure latest security updates & software in internal systems.

The SolarWinds supply chain attack was different from past attacks in which the hackers didn't initiate remote control immediately.

data to integrate and configure latest security updates & software in internal systems. Attacker manipulates manufacturing process by installing rootkit or Hardware based spying components in the system. Types of supply chain attacks: Supply chain attackers generally target the source code, update software's of the system, or build processes of vendor software. A victim can be compromised by any one of the following vectors:

- Third-party software updating process
- Malware installed on connected devices, like HDD, cameras, USB etc.
- New Application installation

SolarWinds supply chain attack 2020-21: The 2020 global supply chain cyberattack is believed to be targeting the IT infrastructure company SolarWinds, which have many global institutions among its clients including critical sectors like power, aviation, space, transport & health services using SolarWinds Software and Hardware. Various cyber agencies of different countries issued advisories to mitigate SolarWinds Orion code compromise which involves disconnection of Windows hosting machines from its enterprise domain, and rebuilding those Windows hosts which are using trusted sources. The SolarWinds supply chain attack was different from past attacks in which the hackers didn't initiate remote control immediately. But the malware lay inactive for two weeks before initiating contact with a command-and-control server through backdoor.

How to prevent supply chain attacks:

- Secure Privileged Access Management.
- Implement an Identity Access Management (IAM).
- Minimise access to sensitive data.
- Monitor vendor network for vulnerabilities.
- Implement Honey tokens as a deception technique
- Adequate training of staff to be aware of latest cyber security trends.
- Identify all potential insider threats.

References:

[1] <https://www.upguard.com>

[2] <http://securityintelligence.com/posts>

[3] <https://threatpost.com/>

ZHtrap Botnet uses Honeypots to find more Targets

BFSI Sector, NCIIPC

Security researchers generally use honeypots as a tool to capture attacks, such as collecting scans, exploits and samples. However, recently, Netlab360 security researchers reported ZHtrap botnet deploying honeypots to find more targets. ZHtrap is a worm and botnet based on Mirai source code and it comes with support for x86, ARM, MIPS and other CPU architectures. Similar like other Mirai source, it targets a wide range of Small Office/Home Office (SOHO) and Internet-of-Things (IoT) devices.

Delivery and Activities: To proliferate, this botnet uses exploits targeting four N-day security vulnerabilities in Realtek SDK endpoints, MVPower DVR, Netgear and a long list of CCTV-DVR devices. ZHtrap identifies new devices to disseminate by scanning randomly generated IP addresses before installing four known exploits or a hard-coded Telnet password list against them. Once installed on a device, it connects to a botnet controller over a Tor node, with all traffic between itself and other devices communicated through another Tor proxy. This botnet is also capable of DDoS attacks and scanning for more vulnerable devices to infect. It has the capability of backdoor functionality which allows the operators to download and execute other malicious payloads.

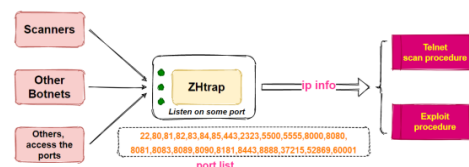
Bots used as honeypots: interesting feature of this botnet is, how it turns infected devices into honeypots to collect IP addresses of devices already infected by some other malware.

ZHtrap has evolved some tricky new features:

- **Instructions:** A checksum mechanism has been added
- **Scanning propagation:** The distinction between real devices and honeypots has been added
- **Encryption algorithm:** A set of multiple XOR encryption algorithms has been redesigned
- **Network Architecture:** It copies some operations of previously exposed botnet.

Remediation:

- Secure configurations are applied to all devices.
- Outdated platforms are separated from rest of the network.
- IT usage policies are reinforced by regular training, to ensure all users know not to open unsolicited links or attachments.
- Remote administration services use strongly encrypted protocols and only accept connections from authorised users or locations.
- Multi-factor Authentication (MFA) and lockout policies to be used where feasible, especially for administrative accounts.



ZHtrap usage of IP collection module

Zhtrap identifies new devices to disseminate by scanning randomly generated IP addresses before installing four known exploits or a hard-coded Telnet password list against them.

Multi-factor authentication (MFA) and lockout policies to be used where feasible, especially for administrative accounts.

- Use Administrative accounts only when there is necessity.
- Systems are regularly monitored, and abnormal activity is investigated, so that a compromise of the network can be detected as early as possible.

References:

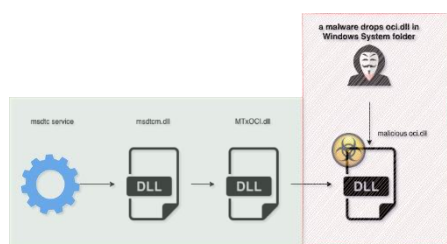
- [1] <https://digital.nhs.uk/cyber-alerts/2021/cc-3793>
- [2] <https://www.bleepingcomputer.com/news/security/new-zhtrap-botnet-malware-deploys-honeypots-to-find-more-targets/>
- [3] <https://blog.apnic.net/2021/05/04/zhtrap-botnet-uses-honeypot-to-harvest-infected-devices/>

Malware Bytes

'Pingback' Malware uses ICMP for Covert Communication

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

A novel Windows malware dubbed as Pingback has been disclosed by researchers. It uses Internet Control Message Protocol (ICMP) for its command-and-control (C2) activities and targets Microsoft Windows 64-bit systems, and uses DLL Hijacking to gain persistence. The malicious file is a 66-KB DLL called oci.dll, an Oracle library (Oracle Call Interface) that exists for supporting and interacting with Oracle databases. Trustwave's researchers identified that it was the Microsoft Distributed Transaction Control (msdtc) service being abused to load the malicious oci.dll. It is suspected that another malware sample, updata.exe is behind both dropping the malicious oci.dll in the Windows "System" folder and configuring msdtc to run on every start-up. According to researchers, the advantage of using ICMP for communications is that Pingback remains effectively hidden from a user as ICMP has no concept of "ports" and uses neither TCP nor UDP. As a result, oci.dll may not be picked up by diagnostic tools like netstat.



Process tree of malicious DLL being loaded by legitimate Windows processes

Source: Trustwave

Unsubscribe Emails Lead to further Spam

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

Scammers have been using fake 'unsubscribe' spam emails to confirm valid email accounts that can be used in future phishing and spam campaigns. Spammers have been sending emails that simply ask- if you wish to unsubscribe or subscribe. These emails do not explain what is to be unsubscribed or subscribed to. The email messages are very basic containing links asking whether you would like to unsubscribe or subscribe. If user clicks on the embedded subscribe/unsubscribe links, it will cause user's mail client to create a new email that will be sent to many different email addresses under the spammer's control. When users send the



above email, they expect to be unsubscribed from further emails but they are actually verifying for the spammers that their email address is valid and being monitored.

Three New Malwares used by SolarWinds Hackers

Source: <https://gbhackers.com/>

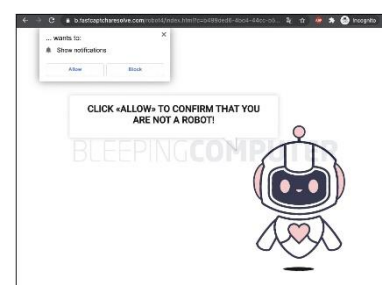
Microsoft have identified three new pieces of malware being used in late-stage activity of SolarWinds supply chain attack that have compromised multiple organisations. These three malwares are GoldMax, Sibot, GoldFinder. Goldmax malware imitates as systems management software. The malware writes an encrypted configuration file to disk using AES-256 encryption algorithm. This AES encrypted data is Base64-encoded using custom Base64 alphabet. Sibot malware is implemented in VBScript. It is used for maintaining access on the infected machine. It downloads and executes payload from remote C2 server. VBScript file impersonates itself as legitimate windows tasks and found stored in registry of the compromised system or in an obfuscated format on disk. Goldfinder is a custom HTTP tracer tool to logs the route or hope that packets take over a network to reach a hard-coded server. This malware sends an HTTP request to a hard-coded IP address and logs the HTTP response to a plaintext log file.

The malware writes an encrypted configuration file to disk using AES-256 encryption algorithm. This AES encrypted data is Base64-encoded using custom Base64 alphabet.

Fake jQuery Files Infect WordPress Sites with Malware

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

Security researchers have found forged version of jQuery Migrate plugin which contains obfuscated code to load malware. Files are jquery-migrate.js and jquery-migrate.min.js injected on dozens of websites. To make detection difficult malicious files are replaced by the original legitimate files present at ./wp-includes/js/jquery/. These malicious jQuery files load analytics.js file with malicious code within. These malicious codes have references to wp-adminuser-new.php which is WordPress administration page. Further code access wpnonce_create-user variable which enforces Cross-Site Request Forgery (CSRF) protections. This gives attacker ability to make forged request on behalf of users. The checkme() function inside the code redirect user's browser window to a malicious URL. It redirects to fake surveys, tech support scams. The network of spam URLs used in the redirect sequence is vast with multiple domains. These URLs have low virustotal detection rate thus performing security scans of websites by relying on signature-based scanning is not sufficient. To make website secure perform security audits and check for anomalies that indicate signs of malicious activity.



Malicious analytics.js file redirects the user to malicious URLs of prompting the allow notifications



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**



SUPERNOVA is used by threat actor to perform reconnaissance, conduct domain mapping, and steal sensitive information and credentials.

CISA Identifies SUPERNOVA Malware during Incident Response

Source: <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-112a>

An Advanced Persistent Threat (APT) actor connected to the entity's network via a Pulse Secure virtual private network (VPN) appliance has been identified which moved laterally to its SolarWinds Orion server, installed malware referred as SUPERNOVA (a .NET webshell). SUPERNOVA is used by threat actor to perform reconnaissance, conduct domain mapping, and steal sensitive information and credentials. The threat actor authenticated to the VPN appliance through several user accounts, which does not have Multi-factor Authentication (MFA) enabled and uses a PowerShell script to decode and install SUPERNOVA. Implement MFA especially for privileged accounts, secure Remote Desktop Protocol (RDP) and other remote access solutions using MFA and "jump boxes" for access, implement the principle of least privilege on data access, deploy and maintain endpoint defence tools on all endpoints, ensure all software including anti-virus solutions are up to date, enable firewall on organisation workstations that is configured to deny unsolicited connection requests.

Havoc Caused by Ransomwares

Source: bleepingcomputer.com, www.enigmasoftware.com, securityaffairs.co

Ransomware is on rise, many ransomwares are attacking organisations for their benefit, some ransomwares are discussed here:

FiveHands ransomware is a variant that uses public key encryption scheme called NTRUEncrypt based on the shortest vector problem in a lattice. This malware also encrypts files in the recovery folder.

AgeLocker ransomware is a high-end data-encrypting Trojan. It uses a new encryption service called Age (Actually Good Encryption). Unlocking files encrypted by this file-locker is difficult.

A final update about the Ragnar Locker ransomware attack has been released by Capcom. Ragnar Locker operators gained access to Capcom's internal network by targeting an old VPN backup device located at the company's US subsidiary. From there, the attacker pivoted to devices and detonated the file-encrypting malware, causing email and file servers to be taken offline.

Greed ransomware belongs to the Xorist ransomware group. It encrypts files in infected systems with .greed extension and demands ransom in exchange for the decryption. This malware mainly spread via spam campaigns presented as "urgent", "important", "priority", and similar, even be disguised as mail from legitimate sources.

Security researchers have discovered a new sample of REvil



Image source: <https://static.dw.com>

Security researchers have discovered a new sample of REvil ransomware that allows adversaries to automate file encryption via Safe Mode after changing Windows passwords.

ransomware that allows adversaries to automate file encryption via Safe Mode after changing Windows passwords. It has been observed that a new Windows Safe Mode encryption mode is added to the REvil/Sodinokibi ransomware which would reboot the device into Safe Mode, where it would perform the encryption of files.

The threat actors are actively deploying Cring ransomware to organisations in the industrial sector. Attackers download Mimikatz utility to steal the credentials of Windows users who logged in to the compromised system after gaining access to the system within targeted network. Upon compromising administrator account of the domain, threat actors could distribute malware to other systems on the same network.

Usagoo ransomware is a virus-extortionist. Once infects, it encrypts and turns all the personal files like documents, images, audio/video files, etc into unreadable. Cybercriminals forced users to pay a ransom in return to the file recovery.

RevengeRAT

Transport Sector, NCIIPC

Aerospace and travel industries are targeted with spear phishing emails that distribute an actively developed loader. Email contains malicious MS Office attachments having an embedded link typically abusing legitimate web services, that downloads a malicious VBScript, which drops the RevengeRAT payload on to the victim's system to steal sensitive information. RevengeRAT also known as Revetrat is a high-risk computer infection that belongs to the class of Remote Access Trojan (RAT). The purpose of this malware is to provide cyber criminals with remote access to the infected machine through a secure encrypted connection and allow them to manipulate it. Once RevengeRAT is installed, the attacker can get access to system services/process/files, spying on the victim's activities, Windows Registry entries and hosts file, log keystrokes, steal account credentials, access other devices (e.g., microphones, webcam), execute shell commands, and so on.

Infection Process:

- This malware is delivered onto the victim's machine using attachment links in phishing emails.
- When the victim opens the decoy file, it displays an image to trick the victim into enabling Microsoft Office macros. It allows RevengeRAT to be installed on the victim's computer via a process including multiple steps with various, different URLs.
- Once RevengeRAT is installed, it will disable Microsoft Defender and try to disable other security content on the victim's computer.

The threat actors are actively deploying Cring ransomware to organisations in the industrial sector.



The purpose of this malware is to provide cyber criminals with remote access to the infected machine through a secure encrypted connection and allow them to manipulate it.

Once RevengeRAT is installed, it will disable Microsoft Defender and try to disable other security content on the victim's computer.

Manage situational perception of the latest threats and perform appropriate Access Control Lists (ACLs).

How to Prevent:

- Keep up-to-date antivirus signatures and engines.
- Conserve operating system patches up-to-date.
- Impair all the File and Printer sharing services.
- Use robust passwords or Active Directory authentication.
- Stop users from installing and operating undesired software applications.
- Execute regular password changes.
- Scan properly before opening e-mail attachments, even if the attachment is required, and the sender appears to be appreciated.
- Browse for and eliminate suspicious e-mail attachments.
- Check the users' web browsing habits; restrict access to sites with unsuitable content.
- Practice caution while using removable media.
- Impair unnecessary services on agency workstations and servers.
- Allow a personal firewall on company workstations, configured to deny undesirable connection requests.
- Examine all software that are downloaded from the Internet prior to administering it.
- Manage situational perception of the latest threats and perform appropriate Access Control Lists (ACLs).

References:

- [1] <https://www.scmagazine.com/home/security-news/phishing/revengerat-and-aysncrat-target-aerospace-and-travel-sectors/>
- [2] <https://www.enigmasoftware.com/revengerat-removal/>
- [3] <https://any.run/malware-trends/revenge>
- [4] <https://www.pcrisk.com/removal-guides/15469-revengerat-virus>
- [5] <https://www.kratikal.com/blog/rat-attack-phishing-attack-that-deploys-two-trojans/>
- [6] <https://www.kratikal.com/blog/rat-attack-phishing-attack-that-deploys-two-trojans/>

DarkSide Ransomware

Power and Energy Sector, NCIIPC

Recently, DarkSide ransomware attack forced Colonial Pipeline (US) to proactively shut down its operations. In this attack DarkSide has stolen over 100 GB of corporate data and has been locking the Colonial Pipeline's computer system. After gaining access to the pipeline company's network, DarkSide actors deployed DarkSide ransomware against the IT network. The Pipeline

company proactively disconnected OT systems to ensure the systems' safety. DarkSide actors try to gain initial access through phishing and exploiting remotely accessible accounts and systems and Virtual Desktop Infrastructure (VDI), Exploit Public-Facing Application and External Remote Services, after gaining access, the DarkSide actors deploy the ransomware to encrypt the files and steal sensitive data. The Subsequent proactive measures are required to be in place to ensure the protection of IT/ OT infrastructure of the organisation against the Ransomware attack:

- Develop and ensure robust network segregation between IT and OT networks.
- Organise Operational Technology assets into logical zones by taking into operational necessity and account criticality.
- Identify OT and IT network inter-dependencies and implement manual controls to conform ICS networks may be isolated if the connections create risk to the safe and reliable operation of OT processes.
- Develop regular data backup on both the IT and OT networks.
- On a regular basis test manual controls in order that critical assets will be kept working if ICS or OT networks need to be taken offline.
- Implement multi-factor authentication for remote access
- Implement Robust spam filters to prevent malicious, Phishing emails from end users.
- Filter & Prevent network traffic to block Inbound and Outbound communications with known malicious IP addresses.
- Update the software, including firmware on IT network assets, operating systems and applications.
- Set antimalware/antivirus programs to perform regular scans of IT network assets using up-to-date signatures.

Implement unauthorised execution prevention by:

- Disable macro scripts from MS Office files transmitted through email.
- Develop application allow listing, which only allows systems to execute programs known and permitted by security policy.
- Develop software restriction policies to prevent programs from executing from common ransomware locations, such as compression/decompression programs, temporary folders supporting popular internet browsers.
- Block & monitor the inbound connections from Tor exit nodes to ports, IP addresses.
- Deploy signatures to identify the inbound connection from Cobalt Strike servers.

If an organisation is impacted by a ransomware incident, following are the recommendations:

- Shutdown and isolated the infected computers or any other computers or devices that shared a network with the infected computers.

DARKSIDE VICTIMS BY MONTH



In this attack DarkSide has stolen over 100 GB of corporate data and has been locking the Colonial Pipeline's computer system.

Identify OT and IT network inter-dependencies and implement manual controls to conform ICS networks may be isolated if the connections create risk to the safe and reliable operation of OT processes.

Isolate the infected system. Isolate the infected system from networks, and disable the computers from the wired & wireless connections.

- Isolate the infected system from networks, and disable the computers from the wired & wireless connections.
- Make sure that backup data is offline and secure. Scan the backup data with an antimalware /antivirus program to check that it is free of malware.

References:

- [1] <https://us-cert.cisa.gov/ncas/alerts/aa21-131a>
- [2] https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html



COAS CHAIR OF EXCELLENCE CENTER FOR LAND WARFARE STUDIES

Dear Sir you are select for COAS chair of excellence. More details in below link.

DIR CLAWS

Link: <https://sharingmymedia.com/files/1More-details.doc>

Note:- Please copy link then paste on google search bar then enter after downloading file click on file if file show blank then click on left side enable content then ok. Please download through laptop.

Maldoc masquerading as a congratulatory notice from CLAWS

Secure the backups. Make sure that backup data is offline and secure. Scan the backup data with an antimalware /antivirus program to check that it is free of malware.

Transparent Tribe APT added new Windows Malware in its Arsenal

Threat Assessment Team, NCIIPC

Transparent Tribe, additionally referred to as APT36 and Mythic Leopard is a Pakistan-sponsored highly prolific group and it primarily attacks Indian military and government personnel for cyber-espionage activities. The group continues to create fake domains mimicking legitimate army and defence organisations as a centre component of their operations. Previous research has specially linked this organisation to CrimsonRAT, but new campaigns display they're expanding their Windows malware arsenal with ObliqueRAT. While targeting Military and defence personnel remain the group's primary objectives, Transparent Tribe is increasingly targeting diplomatic entities, defence contractors, research organisations and conference attendees which indicate that the group is expanding its targeting. Recent research report exposed that the Transparent Tribe uses two types of domains in their various campaigns: fake domains masquerading as legitimate Indian defence and government-associated web sites, and malicious domains posing as content-hosting sites. These domains work together to deliver malware documents distributing CrimsonRAT and ObliqueRAT. While Tactics, Techniques, and Procedures (TTPs) of Transparent Tribe have remained largely unchanged since 2020, but the group maintains to implement new lures into its operational toolkit. The group employs variety of maldoc which shows that it still relies on social engineering as a core component of its operations. Two-pronged approach by Transparent Tribe for registering malicious domains is as under:

Fake domains: Latest research on Transparent Tribe confirms that the group maintains to create malicious domains mimicking entities related to defence organisation as a core component of their operations. It was also discovered that a fake domain, [clawsindia\[.\]com](https://clawsindia[.]com) was registered by the attackers and this domain masquerades as the website for the Centre For Land Warfare Studies (CLAWS), an India based autonomous think tank on strategic studies and land warfare. The legitimate domain for

CLAWS is claws[.]in. The malicious clawsindia[.]com domain was previously hosted on a command and control (C2) for CrimsonRAT which is Transparent Tribe's custom .NET Remote Access Trojan (RAT). However, it became additionally diagnosed a subdomain, mail[.]clawsindia[.]com, hosted on the same IP, suggesting that the attackers are using it as part of a malspam campaign. One of the examples of attackers' maldocs is illustrated below in which they target individuals applying for the CLAWS "Chair of Excellence," an honorary title for those making outstanding research contributions to strategic studies. The victim is encouraged to click on an embedded URL hosted on sharingmymedia[.]com, which then downloads ObliqueRAT, the trojan which is associated with threat activity targeting entities in South Asia. As it is not confirmed how the maldocs were delivered to victims, but it is suspected they were probably sent as attachments to phishing emails based on previous behaviour and targeted nature of threat actor.

Malicious file-sharing domains: Transparent Tribe also keeps on registering domains that appear to be legitimate file and media-sharing services. To host ObliqueRAT, the group has used drivestransfer[.]com, file-attachment[.]com, mediaclouds[.]live, and emailhost[.]network during their operations. There is similarity of the infection chain involving these domains with one described above in which the threat actors use social engineering to convince the victim to download and open the malware hosted on these sites.

Conclusion: Transparent Tribe relies heavily on the use of maldocs to roll out their Windows implants. While CrimsonRAT remains the group's leading Windows implant, their development and distribution of ObliqueRAT in early 2020 indicates they are rapidly expanding their Windows malware arsenal. Email and maldoc lures employed to unfold these implants consist of multiple themes, including conference agendas, honeytrap lures and diplomatic themes. The group continues to primarily target defence personnel in India using two generic theme -fake resumes and military related topics. Transparent Tribe uses generically themed content-hosting domains in addition to malicious domains masquerading as legitimate defence-related websites. So, it is obvious that the group is evolving their TTPs to appear more legitimate by using compromised websites to host malicious artifacts.

References:

- [1] <https://us-cert.cisa.gov/ncas/alerts/aa21-131a>
- [2] https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

Transparent Tribe also keeps on registering domains that appear to be legitimate file and media-sharing services.

Transparent Tribe uses generically themed content-hosting domains in addition to malicious domains masquerading as legitimate defence-related websites.

LockBit Ransomware

Transport Sector, NCIIPC



When executed, the ransomware renames the files with the extension ".abcd" after compromising a tool.

Activate multi-factor authentication and Strong passwords should be implemented.

LockBit could be a new encoding ransomware operating since September 2019 and a recent Ransomware-as-a-Service (RaaS), in development and affiliates join up to distribute the threat within the wild. LockBit ransomware is malicious software intended to block user access to systems in exchange for a ransom financial gain. LockBit will automatically evaluate for valuable targets, spread the infection, and encrypt all accessible systems on a network. This ransomware is employed for highly targeted attacks against transport enterprises and other organisations. As a self-piloted cyberattack, LockBit attackers have made a mark by threatening organisations globally with a number of the subsequent threats:

- Operations disruption with essential functions coming to a sudden halt.
- Extortion for the hacker's gain.
- Data theft and illegal publication as blackmail if the victim doesn't comply.

LockBit threatens to leak the information of their victims to extort payments. Recently (28 Apr 2021), UK rail network was hit by a ransomware attack, which is probably initiated by the Lockbit ransomware gang.

Infection Process: When executed, the ransomware renames the files with the extension ".abcd" after compromising a tool. After this process, a document – "Restore-My-Files.txt" is made. 3 ways to spread:

- Self-spreading within a company instead of requiring manual direction.
- Targeted instead of spread in a very scattershot fashion like spam malware.
- Using similar tools to spread, like Windows PowerShell and Server Message Block (SMB).

Indicators of Compromise:

- Type Indicators
- RegistryKey
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\random-generated-letters & HKCU\SOFTWARE\LockBit
- Ransom note names - Restore-My-Files.txt
- Network IoC- Lockbitks2tvnmwk[.]onion , Ocsip.usertrust[.]com & Crl.usertrust[.]com

How to Prevent:

- Keep up-to-date antivirus signatures and engines.
- Activate multi-factor authentication and Strong passwords should be implemented.

- Reassess and simplify user account permissions.
- Use robust passwords or Active Directory authentication.
- Stop users from installing and operating undesired software applications.
- Clean the Registry for any of the manipulated values (once infected).
- Scan properly before opening e-mail attachments, even if the attachment is required, and the sender appears to be appreciated.
- Browse for and eliminate suspicious e-mail attachments.
- To clean up an infected host, it is crucial to revert each of the steps taken by the payload of the attack.
- Allow a personal firewall on company workstations, configured to deny undesirable connection requests.
- Blacklist the SHA256 of the ransomware.
- Examine all software that are downloaded from the internet prior to administering it.
- Enabling the heuristic, AV, and driver mechanisms.
- If necessary, format the host and install a clean version of Windows.
- Manage situational perception of the latest threats and perform appropriate Access Control Lists (ACLs).

References:

- [1] <https://securityboulevard.com/2020/09/lockbit-malware-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/>
- [2] <https://www.cynet.com/blog/threat-report-lockbit-ransomware/>
- [3] <https://www.information-age.com/merseyrail-likely-hit-by-lockbit-ransomware-attack-123494934/>
- [4] <https://www.kaspersky.com/resource-center/threats/lockbit-ransomware>



Scan properly before opening e-mail attachments, even if the attachment is required, and the sender appears to be appreciated.

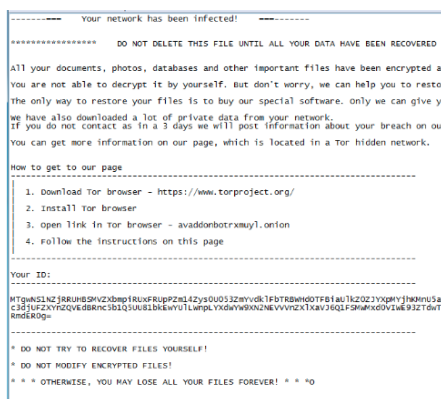
Avaddon Ransomware: Ransomware as a Service

Threat Assessment Team, NCIIPC

Ransomware is a type of malware that encrypts a user or organisation's data so that the files, databases, or applications are not accessible and threatens to publish the victim's data unless a ransom is paid.

Ransomware as a Service: Like Software as a service (SaaS), Ransomware developer provides ransomware variants on lease/subscriptions to their affiliates/customer. RaaS provides people even without much technical knowledge, the ability to launch ransomware attacks just by buying services and paying the developers a percentage of their take. RaaS also provides various customisation features like support, custom ransom notes, the





Avaddon ransom notes contain a unique victim ID and a link to the TOR website at avaddonbotrxmuy[.]onion, which victims must access by a TOR browser.

Secure backups and ensure data isn't accessible for modification or deletion from the system where the info resides.

amount of the payment, and an administration panel to control the server to manage each victim which makes it convenient for buyers who want ready-made ransomware without any specific technical knowledge.

Avaddon Ransomware: An ongoing campaign of Avaddon ransomware is targeting manufacturers, airlines, healthcare organisations, and others. It was first published on Russian language hacking forums as a ransomware-as-a-service and targets windows systems. It uses spear phishing and malspam campaigns to deliver malicious JavaScript files which are often low in sophistication. It was written in C++ and for encryption, it uses a unique AES256 encryption key. During the infection process, It checks the OS language and keyboard layout to verify the victim is not located in the Commonwealth of Independent States (CIS). Analysis of this ransomware reveals common capabilities of ransomware like encryption, persistence through registry keys and windows scheduled task, activity control, and anti-analysis. Avaddon ransom notes contain a unique victim ID and a link to the TOR website at avaddonbotrxmuy[.]onion, which victims must access by a TOR browser. This website provides technical support, negotiate with victims via a web chat functionality, post data leaks, and receive ransomware payments from victims. When victims enter their IDs, they receive instructions to pay the ransom and decrypt their data. Avaddon threat actors demand ransom payment via Bitcoin (BTC), with a mean demand of BTC 0.73 (approximately USD 40,000) with the lure of a decryption tool offered (Avaddon General Decryptor) if payment is made.

Recommended mitigations:

- Install endpoint security software.
- Back-up critical data offline regularly.
- Secure backups and ensure data isn't accessible for modification or deletion from the system where the info resides.
- Use two-factor authentication with strong passwords.

References:

- [1] <https://www.cyber.gov.au/acsc/view-all-content/advisories/2021-003-ongoing-campaign-using-avaddon-ransomware>
- [2] https://agileblue.com/wp-content/uploads/2021/05/flash_avaddon_ransomware.pdf
- [3] https://www.databreachtoday.eu/alerts-avaddon-ransomware-attacks-increasing-a-16563?utm_medium=email&_hsmt=126622296&_hsenc=p2ANqtz-97TV23mr0tr5moNJSQ-BZUNi0rLaV8_R4Y7281HfjFjQhlcR6gBoX3BfacdzQcGOWsYAHbSH6YWuCNrrqbYA76WMU3g&utm_content=126622296&utm_source=hs_email

[4] <https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware.html>

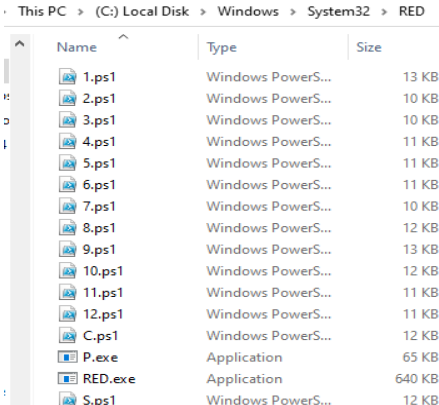
Epsilon Red Ransomware

S&PE Sector, NCIIPC

Epsilon Red is a new form of ransomware that has been found targeting unpatched Microsoft Exchange servers to encrypt machines across the network. The name of Epsilon Red came from a pop-culture referring to a character in the Marvel Universe comic books, a Russian super-soldier with four tentacles that can breathe in space. It is also described as bare-bones ransomware. The ransomware was designed to scan the systems for files and folders to encrypt and then perform the actual encryption. The remaining tasks are carried out by 12 PowerShell scripts that prepare the machine for the actual encryption payload. It is written in an open-source programming language Golang (Go) which described as easy to build simple, reliable and efficient software. It is preceded by a set of unique PowerShell scripts. It is known that an organisation unpatched Microsoft Exchange server was the initial entry point, but it is still unclear if the attackers exploited the ProxyLogon exploit or another flaw. Then the attackers used Windows Management Instrumentation (WMI) to install other software onto machines that are inside the network. During the attack period, the threat actors launch a series of PowerShell scripts named 1.ps1 to 12.ps1 and some of them are named with a single letter of alphabet, that prepare the attacked machines for the final ransomware payload and ultimately encrypts the files. The automated management and process of PowerShell scripts were created and triggered by a PowerShell script named RED.ps1 that will be executed on the target machines using Windows Management Instrumentation (WMI) to install software. The script retrieves and unpacks into the system32 folder a .7z archive file that contains the rest of the PowerShell scripts that ultimately deploy Epsilon Red executable. It also makes Scheduled Tasks that run the scripts numbered from 1 to 12 but skips 7 and 8. Further it creates tasks for scripts named "S" and "C".

Effects of Epsilon Red Ransomware:

- It kills processes and services for security tools, backup programs, databases, Microsoft Office apps and email clients.
- It steals password hashes contained in the Security Account Manager file and deletes all Volume Shadow Copies.
- It deletes Windows Event Logs and disables Windows Defender.
- The ransomware suspends processes, uninstalls security tools and expands permissions on the system.



Name	Type	Size
1.ps1	Windows PowerS...	13 KB
2.ps1	Windows PowerS...	10 KB
3.ps1	Windows PowerS...	10 KB
4.ps1	Windows PowerS...	11 KB
5.ps1	Windows PowerS...	11 KB
6.ps1	Windows PowerS...	11 KB
7.ps1	Windows PowerS...	10 KB
8.ps1	Windows PowerS...	12 KB
9.ps1	Windows PowerS...	13 KB
10.ps1	Windows PowerS...	12 KB
11.ps1	Windows PowerS...	11 KB
12.ps1	Windows PowerS...	11 KB
C.ps1	Windows PowerS...	12 KB
P.exe	Application	65 KB
RED.exe	Application	640 KB
S.ps1	Windows PowerS...	12 KB

Epsilon Red Ransomware Files

The ransomware was designed to scan the systems for files and folders to encrypt and then perform the actual encryption. The remaining tasks are carried out by 12 PowerShell scripts that prepare the machine for the actual encryption payload.

It kills processes and services for security tools, backup programs, databases, Microsoft Office apps and email clients.

Delete all programs and files in your system related to Epsilon Red ransomware

Sources and Prevention of Epsilon Red Ransomware:

- As the entry point for this attack appears to be an Exchange server that is vulnerable to the Proxy Logon exploit chain, it may be prevented by patching internet facing Exchange servers as quickly as possible.
- It is not safe to open/download attachments or links received from unknown sources without being sure that it is safe.
- One more way to prevent malicious programs from causing damage is to have a reputable and reliable anti-spyware or antivirus suite on the operating system installed and regularly scan it for threats.

Suggestive steps for removal of Epsilon Red ransomware:

Step-1: Boot PC in Safe Mode.

Step-2: Clean any registry-entries, created by Epsilon Red ransomware

Step-3: Scan for programs or files potentially related to Epsilon Red by using Anti-Malware Tools.

Step-4: Delete all programs and files in your system related to Epsilon Red ransomware

Step-5 (Optional): Try to Restore Files Encrypted by Epsilon Red ransomware.

References:

- [1] <https://news.sophos.com/en-us/2021/05/28/epsilonred/>
- [2] <https://heimdalsecurity.com/blog/epsilon-red-ransomware-goes-after-unpatched-microsoft-exchange-servers/>
- [3] <https://blog.knowbe4.com/new-ransomware-strain-epsilon-red-is-reported>
- [4] <https://www.computips.org/how-to-remove-epsilon-red-ransomware-and-decrypt-epsilon-red-files/>

Learning

Tips on Enhancing Supply Chain Security

Source: <https://www.bankinfosecurity.in/>

The United States National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) have released a report that provides guidance to enhance supply chain security called "Defending Against Software Supply Chain Attacks". This report provides in-depth recommendations for software vendors and customers also provide important steps for prevention, mitigation and resilience of software supply chain attacks. NIST's frameworks supply chain risk management recommendations includes:

- Establish a set of security controls for all suppliers based on the



criticality of the supplier and the permissions granted to the information and communications technology.

- Use supplier certifications to ascertain whether a supplier incorporates secure software development practices throughout all life cycle phases, actively identifies and discloses vulnerabilities and maintains a product vulnerability response program.
- Ensure that vendors enforce supply chain security requirements that meet the standards used by the purchasing organisation.

The report says vendors in the supply chain should:

- Perform in-house and third-party code review, analysis and testing.
- Configure software so that it is secure at the time of installation.
- Use properly configured build processes to improve the security of executable code.

Work From Home: Wi-Fi Security Tips

Source: <https://channeleye.media/>

People generally think that a hacker would not be interested in their home network. But everyone has something that is valuable to attackers- personal information, bank details, and financial data. While working from home, it is important to remember that a skilled attacker can easily access the network from one's personal computer or connected device to their work laptop, and possibly from there to the whole network of the company. Here are few tips to ensure the security of Wi-Fi network:

Apply updates: It is advised to apply patches and updated to all access points, routers and modems that are used for home network, as well as all devices that could be connected to it.

Check encryption settings: It is recommended to use at least WPA2-PSK (AES) encryption. Never use Wired Equivalent Privacy (WEP), as the encryption system it uses was completely cracked many years ago.

Use of proper password: An obvious password would make it easy for uninvited people to connect to the network.

Check who's on the network: Check which devices accessed the Wi-Fi network recently, if there are unknown devices accessing the network, disconnect them.

Review the IoT devices: Only connect devices that you really need to have online.

This report provides in-depth recommendations for software vendors and customers also provides important steps for prevention, mitigation and resilience of software supply chain attacks.



While working from home, it is important to remember that a skilled attacker can easily access the network from one's personal computer or connected device to their work laptop, and possibly from there to the whole network of the company.

Ransomware Defence is Catching Up with Ransomware Attack

Source: <https://hostnoc.com/>

Ransomware attacks are evolving at a rapid pace instead of targeting large-scale businesses, it's now targeting critical infrastructures.

Ransomware attacks are evolving at a rapid pace instead of targeting large-scale businesses, it's now targeting critical infrastructures. Ransomware defence needs to continue to evolve. The ways in which ransomware defence is improving with a ransomware attack:

Hunt and Prevent: the ransomware defence mechanism should be capable of predicting it, anticipate the risk and act before the ransomware attack can wreak havoc.

Backup: Backing data regularly is one of the most effective ways to protect business from ransomware attacks.

Network Segmentation: Ransomware moves throughout the network laterally and encrypts more data. Network segmentation can isolate network traffic and apply limits or limits or prevent access between different network segments.

Growing Awareness: Cybersecurity awareness of employees helps in protecting themselves from cyber-attacks.

Redefining Policies: It is required to change the company policies in order to protect the organisation from ransomware threats.

Ransomware Task Force Framework

Source: <https://securityandtechnology.org/>



To effectively disrupt such attacks government and industry stakeholders must work collaboratively to reduce the profitability of criminals.

Ransomware is a national security risk along with financial crime it threatens hospitals, businesses and government across the globe. The recommendations by over 60 experts from industry, government, law enforcement, civil society, and international organisations forms a comprehensive framework to reduce ransomware attack. Ransomware Task force framework helps policymaker and industry leaders to take system-level action through potential legislation, funding new programs or launching new industry-level collaborations. This framework is organised for four goals:

Deter ransomware attacks: Number of actors capable of conducting ransomware attack is large and growing day by day. To discourage such attacks deterrence must be multilayered and rely on all instruments of national power. It is recommended to raise the priority of ransomware within the intelligence community and designate it as national security threat and exerting pressure on nation-states that act as safe-heavens for ransomware activity.

Disrupt ransomware business model: Ransomware basically is a financially motivated crime that will continue as profit occurs to attackers. To effectively disrupt such attacks government and industry stakeholders must work collaboratively to reduce the

profitability of criminals. Disrupting payment systems and infrastructure that facilitates such attack are actions that can be taken.

Help organisations prepare for ransomware attacks: Any organisations can become victim to ransomware. Majority of organisation lack an appropriate level of preparedness to defend against ransomware attacks. As threat is evolving and coming with its advance version now it becomes mandatory to increase awareness and build defences that will be effective at scale. It is recommended to develop a clear, actionable framework for ransomware mitigation, update cyber-hygiene regulations and standards, run awareness campaigns and tabletop exercises.

Respond to ransomware attack effectively: For a victim organisation ransomware attack can be stressful. In such cases crucial decisions need to take under intense pressure. To improve organisation's ability to respond to ransomware attacks more effectively government and industry leaders should increase the resources and information available to ransomware victims. It is recommended to create ransomware emergency response authorities, organisations and incident response entities should share ransomware payment information with a national government prior to payment.

It is recommended to create ransomware emergency response authorities, organisations and incident response entities should share ransomware payment information with a national government prior to payment.

Defending against Web Scraping Attacks

Source: <https://darkreading.com>

Web scraping is an old method in which bots extract data and content from website. It is a kind of threat which organisations frequently underestimate. Scrapping document metadata is also useful for detecting internal hostnames and software versions in use at targeted company. With this information attacker can customize its attack to exploit vulnerabilities specific to company and it also helps in victim reconnaissance. There are several ways to reduce the risk of web scrapping:

- Organisations should audit their websites to make sure that they are not unintentionally exposing sensitive information through published documents or information stored in back-end databases.
- Organisation should have a process to strip metadata from documents before they are published externally. They should not reveal usernames, file paths, print queues and software versions.
- Password-reset pages contain verbose messages that disclose if a submitted username is valid or not. In such cases pages should return generic messages. The key is that page should not indicate whether the account or information is valid.

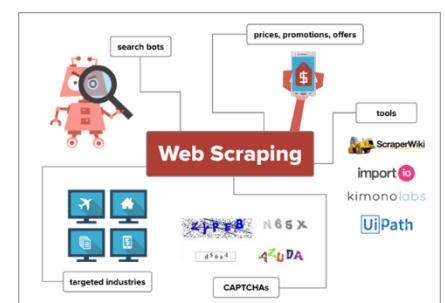


Image source:
<https://miro.medium.com/>

Organisations should audit their websites to make sure that they are not unintentionally exposing sensitive information through published documents or information stored in back-end databases.

- Rate limiting and CAPTCHAS are standard defences against scraping but attacker can also bypass it by CAPTCHA-solving services or rotating through a list of IP addresses. These methods can make web scraping difficult but could not stop it.

Defending against Software Supply Chain Attacks

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

Threat actors are using various techniques to execute software supply chain attacks. The three common techniques used are:

Hijacking Updates: Threat actors can hijack a software update by infiltrating vendor's network and inserting malware into it.

Undermining Codesigning: Attackers can undermine codesigning by self-signing certificates, breaking signing systems or exploiting misconfigured account access control.

Compromising Open-source code: Open-source code comprises occur when threat actors insert malicious code into publicly accessible code libraries.

Organisations are vulnerable to such attacks due to two major reasons: first, many third-party software products require privileged access and secondly, third-party software requires frequent communication between a vendor's network and vendor's software product located on customer networks. Consequences of software supply chain attack is severe. Threat actors can use the compromised software vendor to gain privileged and persistent access to a victim network. Depending on threat actor's intent and capability malware may allow threat actor to conduct malicious activities like financial theft, monitoring organisations, disabling networks or systems.

Recommendations: Organisation acquiring software and other ICT products and services should consider its use in the context of risk management program. Key practices for establishing a Cyber Supply Chain Risk Management (C-SCRM) approach:

- Integrate C-SCRM across the organisation.
- Establish a formal C-SCRM program.
- Know and manage critical components and suppliers.
- Understand the organisation's supply chain.
- Closely collaborate with key suppliers.
- Include key suppliers in resilience and improvement activities.
- Assesses and monitor throughout the supplier relationship.
- Plan for the full life-cycle.

These practices can assist in preventing, mitigating, and responding to software vulnerabilities that might be introduced through the cyber supply chain and exploited by malicious actors.

Risk Management Program Some Simple Steps

1. Identify your key mission or business processes—what essential services do you provide or what drives your revenue?
2. Maintain an inventory of your organization's current and future software licenses
3. Research and document how each software license is supported by its supplier (e.g., Are patches provided? Does the supplier offer periodic email updates about the product?)
4. Understand how your software (current or future purchases) supports or otherwise relates to your key processes
5. Document how you would plan to address software for which a vulnerability is disclosed

Threat actors can hijack a software update by infiltrating vendor's network and inserting malware into it.

Threat actors can use the compromised software vendor to gain privileged and persistent access to a victim network.

Cyber Security in Energy Sector

Team Power and Energy Sector, NCIIPC

Recent ransomware attack on pipeline has once again exposed the systemic vulnerability of the energy industry to cyber-attacks. The cybersecurity risks are increasing day by day due to IT/OT convergence. The energy sector is vulnerable to cyber-attack mainly due to three reasons. First, state actor seeking to cause security and economic dislocation of the country. Secondly, vulnerability utilises expansive and increasing attack surface, arising from their geographical and organisational complexity. Lastly the electric-power and gas sector unique inter dependencies between physical and cyber infrastructure make companies vulnerable to exploitation. The following proactive measures are required to be in place to ensure the protection of IT/ OT infrastructure of the organisation against the Ransomware attack.

- Ensure 24 x 7x 365 monitoring of your network with advanced intrusion detection systems (IDS).
- SCADA devices and software should be secured to the most strengthened physical and logical controls.
- SCADA systems should record all device accesses and commands, especially those involving inbound and outbound connections of the remote sites.
- Radio communications commonly used in SCADA systems are to be secured with proper configuration.
- An antivirus with the best ransomware protection to be installed.
- Take Backup of critical systems regularly.
- Restrict Account Privileges: Ensure system is running in least privileges mode and users are administratively prohibited from installing unauthorised software.
- Disable the use of USB and other removable storage media devices or removable media usage policy may be implemented.
- Disable macros in Microsoft Office Applications.
- Security software: Deploy personal Firewalls, Antivirus, Next Generation Firewall, IDS/ IPS/ UTM and other security related software and update them regularly. Regularly update the OS patches.
- Avoid using unsupported operating system.
- Carry out Vulnerability Analysis Penetration Testing (VAPT) and information security audit in respect of Information & Infrastructure of the Organisation.
- Disable macros in Microsoft Office Applications.
- Prepare your security team to monitor, detect and respond to OT-specific cyber incidents, without risking dangerous impacts.
- Remote maintenance of critical systems may be avoided.

The following reactive measures are required to be taken immediately after a ransomware attack on Information



Deploy personal Firewalls, Antivirus, Next Generation Firewall, IDS/ IPS/ UTM and other security related software and update them regularly. Regularly update the OS patches.

Disconnect the affected system from the rest of network and internet immediately to prevent the malware from further spread.

Review the logs of IDS, IPS, Firewall, UTM and other Security devices for identification of Malware, source of attack and possible compromised systems within the network.

Infrastructure:

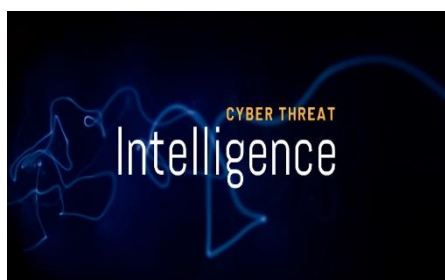
- Disconnect the affected system from the rest of network and internet immediately to prevent the malware from further spread.
- Run antivirus and other security tools as an attempt after identifying and removing the Malware, if possible.
- Review the logs of IDS, IPS, Firewall, UTM and other Security devices for identification of Malware, source of attack and possible compromised systems within the network.
- Change Login passwords of online accounts and other networks.
- Contact Law Enforcement agencies.

References:

- [1] <https://www.bbc.com/news/business-57050690>
- [2] <https://www.mckinsey.com/business-functions/risk/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities>
- [3] <https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html>
- [4] <https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/>
- [5] https://www.oilandgasiq.com/events-cybersecurity-in-energy-and-utilities/?mac=CSIQ_ArticleIndex_EOI_Title_Listing&utm_medium=Portal&utm_source=cyber-security-hub

Dark Web Cyber Threat Intelligence

Threat Assessment Team, NCIIPC



In recent years, cyberattack methods have become highly sophisticated each day. It can also be said that against cyber criminals' people can only fight defensively. Current techniques for dealing with cyber-attacks are reactive, meaning once an attack occurs then cyber professionals take actions. This is no longer acceptable because cyber breaches leak secrets and information which damage entities. So, it is need of the hour to predict cyberattacks and take appropriate actions in advance, and the use of intelligence can play a key role to predict cyber-attacks. Hackers spend a lot of time-exchanging information on online communities like darknet. The darknet is a kind of network with restricted access which allows people to stay anonymous for legal and illegal purposes. Attacker's presence in online forums may contain data that may help us in the discovery of cyber threat intelligence.

Cyber Threat Intelligence: The world is getting more connected,

automated and run by computers and smart devices creating the cyberspace. Therefore, it is crucial to monitor, collect and analyse data related to security threats and vulnerabilities in cyberspace. Cyber Threat Intelligence (CTI) is knowledge and understanding of these threats. The adaptation of cyber threat intelligence is very important in getting ahead of attackers. In cyber security field, monitoring and collection of data is the first step in efforts to defend against cyber-attacks which generates a big data associated with these security events. Currently cybersecurity teams have had challenges in making use of security related large data and are looking towards artificial intelligence/machine learning to help them parse and analyse this data and discover intelligence about the threats and possible attacks. The first element of the Cyber Threat Discovery from Dark Web is the identity of a threat actor such as a person, an organisation, or a nation state to find any strategy, tools, tactics, techniques, and procedures expected to be used. The other elements are motivations, strategy, goals, target, TTPs (Tactics, techniques, and procedures), indicators of compromise (IOCs) and courses of action.

The value of Dark Web Sources for Cyber Threat Intelligence: There's no hesitation in saying that researchers can use the dark web to obtain highly valuable cyber threat intelligence, quite often relevant to a broad spectrum of potential targets, both individuals and organisations which is not accessible through conventional monitoring. For example, healthcare organisations can identify compromised patient records and records and financial institutions can analyse stolen payment information for common point of purchase, and mitigate against future fraudulent charges.

Hacker Forum Analysis: Hacker forums are mostly found on the Darknet. Forum posts are written in natural language, so it is very difficult for a computer to find out sensible information without human assistance. One method of analysing forum posts is sentiment analysis which is a process of determining the positive or negative tone of a piece of text. In addition, forum post can also be analysed using keyword searches. To detect a potential threat, analysis of keywords such as worms, virus and malware can really help. Another important approach for CTI detection is to use analytics and machine learning.

Machine Learning for CTI discovery: Machine learning is the process of teaching machines to see patterns in data which can be used as cyber threat intelligence to counter cyberattacks beforehand. There are mainly 2 types of machine learning algorithms: supervised and unsupervised learning algorithms. Sometimes a mix of supervised learning and unsupervised learning known as semi-supervised learning is mainly utilised when the data is not completely labelled. The machine learning algorithms used for CTI discovery include decision tree, support vector machine

Cyber threat intelligence (CTI) is knowledge and understanding of these threats. The adaptation of cyber threat intelligence is very important in getting ahead of attackers.

The first element of the Cyber Threat Discovery from Dark Web is the identity of a threat actor such as a person, an organisation, or a nation state to find any strategy, tools, tactics, techniques, and procedures expected to be used.

Contents of forum posts are to be analysed to get an insight on understanding hackers' identity, strategy, targets, motivations, tactics, etc. that can help security professionals prevent attacks.

The key to further progress in this area is continued evolution and automation so that such cyber threat intelligence can be made available to a wide variety of organisations to drive security decisions and protect their critical infrastructure more effectively.

and naïve Bayesian, and were successful in analysing textual dataset. Furthermore, Convolutional Neural Networks is up there, and a natural language processing approach, analysing character n-grams vs word n-grams is an interesting point to explore.

Potential Barriers to Dark Web Intelligence: We've seen the potential value of information on the dark web, but discovery of this intelligence comes with its challenges. Useful references to ongoing and emerging cyber threats can be found, but they exist among hundreds of thousands of other dark web conversations in hundreds of underground communities. This is an overwhelming amount of largely irrelevant information that risks wasting more resources rather than getting the possible outputs. Another challenge is access to many of these communities is closely guarded and you may need to prove your capabilities or motivations to get into them. Finally, although the internet is global, many of the dark marketplaces exist in their own geographies and therefore, their own local languages, making understanding references to threats and targets difficult to identify and understand.

Conclusion: Threat intelligence gathered from the dark web is a window into the methods, motivations and tactics of threat actors. Having the time and resources to collect data from numerous sources, analyse, and combine intelligence manually is a cumbersome task. There are service providers who will conduct dark web research and can deliver intelligence reports, but this does introduce the risk of a time lag, or that the information provided might not be directly related to your business, industry, or technologies. In order to make the best use of dark web intelligence, we want to be alerted only when new and pertinent information appears, and we must be able to quickly determine if what's appeared requires further investigation or escalation. Using intelligence to assess risk will ultimately add an extra layer of confidence in security and will surely help in efficient decision making. The key to further progress in this area is continued evolution and automation so that such cyber threat intelligence can be made available to a wide variety of organisations to drive security decisions and protect their critical infrastructure more effectively.

References:

- [1] <https://easychair.org/publications/open/MK31>
- [2] <https://go.recordedfuture.com/hubfs/white-papers/dark-web.pdf>
- [3] https://www.researchgate.net/publication/329367473_DarkWeb_Cyber_Threat_Intelligence_From_Data_to_Intelligence_to_Prediction

Port Cyber Security

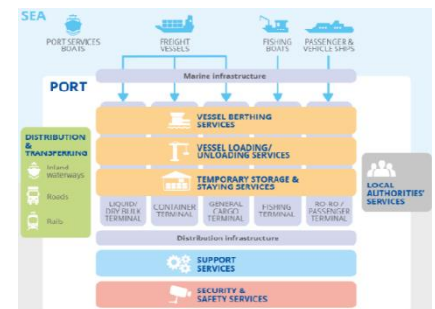
Transport Sector, NCIIPC

The global digitalisation and recent policies and regulations require ports to face new challenges with respect to information and communication technology (ICT). Ports are dependent to trust more on technologies to be more competitive, follow with some standards and policies and optimise operations. This brings new stakes and challenges in cybersecurity, both in the Information Technologies (IT) and Operation Technologies (OT) worlds. Main challenges that the ports are presently facing to implement cybersecurity measures are as follows:

- Deficiency of digital culture in the port ecosystem, in which some stakeholders are still conservative. New trends such as digitisation and IoT initiatives are colliding with the conservative nature of the maritime industry, but are becoming more and more adopted. In this environment, the cyber security needs and best practices of these initiatives are not considered as a priority by stakeholders who are looking at technology adoption.
- Lack of awareness and training regarding cybersecurity: IT and OT bring new challenges with regards to cybersecurity that port stakeholders often do not fully anticipate and master.
- Legacy of some systems and practices, especially regarding systems managing navigation data and OT systems which can be old and vulnerable.
- Technical complexity of port IT and OT systems: The port stakeholders use different systems that are developed, managed and maintained by different teams or entities.
- IT and OT convergence and interconnection: Usually, OT systems are more vulnerable than IT systems, because they are separated from IT systems and networks. But IT and OT systems and networks became more and more dependent and interconnected, exposing OT systems to increases the risks.
- Strong inter-dependencies between port systems and external services from other sectors (e.g., energy) that introduce inter-dependency cybersecurity risks.
- New cyber risks resulting from the digital transformation of ports.
- Supply chain challenges
- Lack of time and budget allocated to cybersecurity.
- Complexity of the port ecosystem due to the number and diversity of stakeholders taking part in port operations.
- Need to find a right balance between business efficiency and cybersecurity.
- Lack of regulatory requirements regarding cybersecurity
- Difficulty to stay up to date with the latest threats.

Key Cyber Attack Scenarios:

- Compromising of critical data to steal high value cargo or



Ports are dependent to trust more on technologies to be more competitive, follow with some standards and policies and optimise operations.

Usually, OT systems are more vulnerable than IT systems, because they are separated from IT systems and networks. But IT and OT systems and networks became more and more dependent and interconnected, exposing OT systems to increases the risks

Supply chain management: Security measures to understand and secure the relationship with third parties in regards with cybersecurity and ensure legit access to port systems.

allow illegal trafficking through a targeted attack.

- Spreading of ransomware leading to a total termination of port operations.
- Compromise of port community system for handling or stealing of data.
- Compromise of OT system create a major accident in port areas.

Recommendations:

- IT and OT physical protection: Security measures to prevent unauthorised physical access to IT and OT systems.
- Endpoint protection and lifecycle management: Security measures related to the protection of IT end devices such as laptops, desktops, tablets, mobile phones etc.
- Vulnerabilities management: Security measures to ensure systems keep up to date and protected from vulnerabilities.
- Human Resource Security: Security measures to ensure good mastery of IT and OT operations and awareness of all employees.
- Supply chain management: Security measures to understand and secure the relationship with third parties in regards with cybersecurity and ensure legit access to port systems.
- Detection and Incident response: Security measures to define processes regarding detection and response of security incidents occurring in the port ecosystem.
- Control and auditing: Security measures to control IT and OT compliance to ISSP and to security best practices.

References:

- [1] <https://www.sciencedirect.com/book/9780128118184/port-cybersecurity>
- [2] <https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector>
- [3] <https://www.cisa.gov/publication/port-facility-cybersecurity-risks>
- [4] <https://www.packetlabs.net/maritime-port-cybersecurity/>

Overcoming Cyber Threats in 5G Infrastructure

Telecom Sector, NCIIPC

In many countries the deployment of 5G has started. With faster connectivity, ultra-low latency, greater network capacity, 5G will enable large-scale connections, capabilities, and services that can produce more opportunities in areas such as healthcare, manufacturing and transport. However, these capabilities enable 5G networks an attractive target for cyber criminals and foreign opponents to exploit for valuable information and intelligence.



Security risks in 5G network: Although 5G is vulnerable to many of the same cybersecurity risks found in today's existing telecommunications and enterprise networks, it's also subject to new avenues of attack against core network services due to deployment of more complex technologies and operations. Generally, there are three main concerns, why 5G networks are sensitive to cybersecurity risks:

- 5G connects the virtual and real worlds: 5G Technology is based on distributed network architecture, which exposes new attack surfaces and leads to challenges in cybersecurity management. Moreover, the connection between virtual and real worlds by 5G means If a particular network infrastructure is compromised, the consequence will not only be limited in the digital world but also attackers can target connected physical devices such as sensors and cameras and enable them to be taken over and used for distributed denial-of-service (DDoS) attacks.
- 5G is linked through Application Programming Interface (APIs): 5G leverages APIs to enable communications between service functions. Insecure APIs can expose services to attack and place the entire 5G network at risk. For example, latest attack of SolarWinds, NotPetya and CCleaner shows that an attack on a single APIs could compromise the entire infrastructure.
- 5G is linked with enterprise, industrial and IoT services: As 5G expands to incorporate advanced enterprise, industrial, and IoT use cases, breaches can put Critical Infrastructure services at greater risk. The more complex 5G networks make it a larger target for hackers. Therefore, the impact of 5G cyber risks won't be limited to networks providers and users but much larger systems.

5G cybersecurity policy going forward: To build a safe and secure 5G networks, the authorities need to adopt zero-trust frameworks. The end-to-end protecting and monitoring mechanisms of the zero-trust framework will make sure that every activity on the 5G network is secure. A cybersecurity system using this framework should have following characteristics:

- Limiting access to all interactions
- Regulating all interactions
- Partitioning assets through small segments
- Regularly monitoring security systems

References:

- [1] <https://www.securitymagazine.com/blogs/14-security-blog/post/94816-managing-the-5g-risks-in-an-unified-and-standardized-way>
- [2] <https://www.cpomagazine.com/cyber-security/overcoming-cyber-threats-in-a-5g-world/>

5G Technology is based on distributed network architecture, which exposes new attack surfaces and leads to challenges in cybersecurity management.

5G leverages APIs to enable communications between service functions. Insecure APIs can expose services to attack and place the entire 5G network at risk.

To build a safe and secure 5G networks, the authorities need to adopt zero-trust frameworks. The end-to-end protecting and monitoring mechanisms of the zero-trust framework will make sure that every activity on the 5G network is secure.

- [3] <https://www.itproportal.com/features/the-cybersecurity-risks-associated-with-5g-networks-and-how-to-manage-them/>
- [4] <https://www.cisa.gov/blog/2021/05/10/securing-5g-infrastructure-cybersecurity-risks>
- [5] <https://www.5gradar.com/features/5g-security-5g-networks-contain-security-flaws-from-day-one>

Vulnerability Watch

Multiple Vulnerabilities in Cisco Jabber

Source: <https://nvd.nist.gov/vuln/detail/CVE-2021-1411>

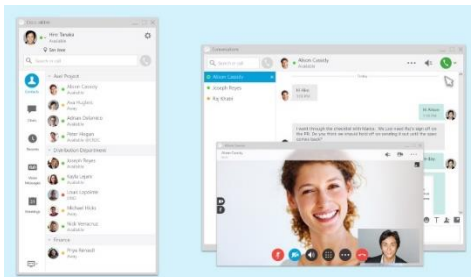


Image Source: <https://nextpointe.com/>

Multiple vulnerabilities in Cisco Jabber for Windows, MacOS, and mobile platforms have been discovered which could allow an attacker to execute arbitrary programs on the underlying operating system with elevated privileges, intercept protected network traffic, access sensitive information or cause a Denial of Service (DoS) condition. These vulnerabilities are CVE-2021-1411 (CVSSv3 score of 9.9), CVE-2021-1417 (CVSSv3 score of 6.5), CVE-2021-1418 (CVSSv3 score of 6.5), CVE-2021-1469 (CVSSv3 score of 7.2) and CVE-2021-1471 (CVSSv3 score of 5.6).

Critical Vulnerability in Xstream

Source: <https://nvd.nist.gov/vuln/detail/CVE-2021-21345>

This vulnerability may allow a remote attacker to execute commands of the host who has sufficient privileges only by manipulating the processed input stream.

A critical vulnerability (CVE-2021-21345 with CVSSv3 score of 9.9) has been discovered in Xstream, which is a Java library to serialise objects to XML and back again. The affected versions are 1.4.16 or before. This vulnerability may allow a remote attacker to execute commands of the host who has sufficient privileges only by manipulating the processed input stream. This could be avoided by following the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types or by using at least version 1.4.16 where users could rely on the Stream's default blacklist of the Security Framework.

Vulnerability in Rockwell Automation FactoryTalk Services Platform

Source: <https://nvd.nist.gov/vuln/detail/CVE-2020-14516>



Image Source: <https://lh3.googleusercontent.com/>

A critical vulnerability (CVE-2020-14516 with CVSSv3 score of 10) has been discovered in Rockwell Automation FactoryTalk Services Platform. The vulnerability exists in the implementation of the SHA-256 hashing algorithm with FactoryTalk Services Platform which prohibits the user password from being hashed properly. The affected versions are 6.10.00 and 6.11.00.

Critical Vulnerability in Fastify

Source: <https://nvd.nist.gov/vuln/detail/CVE-2021-21321>

A critical improper input validation vulnerability (CVE-2021-21321 with CVSSv3 score of 10) has been reported in fastify-reply-from before version 4.0.2. fastify-reply-from is a npm package that is a fastify plugin to forward the current http request to another server. This vulnerability allows to escape the prefix of the proxied backend service, by crafting a specific URL. It is possible to access "/priv" on the target service, if the base URL of the proxied server is "/pub/". This is fixed in version 4.0.2.

This vulnerability allows to escape the prefix of the proxied backend service, by crafting a specific URL.

Multiple Critical Flaws in Eaton Intelligent Power Manager

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

Multiple vulnerabilities have been identified in Eaton Intelligent Power Manager (IPM). CVE-2021-23277 is an Eval Injection flaw which may allow an attacker to control input to the function and execute attacker-controlled commands. CVE-2021-23279 is an Improper Input Validation flaw which allows an attacker to send specially crafted packets to delete the files on the system where IPM software is installed. CVE-2021-23280 is an Arbitrary File Upload flaw which allows an attacker to upload malicious code or execute any command using specially crafted packet. CVE-2021-23281 is a Code Injection flaw which allows attackers to send specially crafted packet to make IPM connect to rouge SNMP server and execute attacker-controlled code. Versions prior to 1.69 are affected by these vulnerabilities. CVE-2021-23277, CVE-2021-23279 and CVE-2021-23281 have CVSSv3 Score of 10 and CVE-2021-23280 has CVSSv3 Score of 9.9.



Powering Business Worldwide

CVE-2021-23279 is an Improper Input Validation flaw which allows an attacker to send specially crafted packets to delete the files on the system where IPM software is installed.

Critical Flaw in SAP Commerce

Source: <https://nvd.nist.gov/vuln/detail/CVE-2021-27602>

Code Injection vulnerability (CVE-2021-27602) has been identified in SAP Commerce. Backoffice application allows authorized users to create source rules which are translated to drools rule. Successful exploitation may allow an attacker with this authorization to inject malicious code in the source rules and perform remote code execution. Affected versions are 1808, 1811, 1905, 2005, 2011. It has CVSSv3 Score of 9.9.



Critical Vulnerability in QNAP NAS Being Exploited

Source: www.qnap.com, <https://nvd.nist.gov/vuln/detail/CVE-2021-28799>

An Improper Authorization vulnerability has been reported to affect QNAP NAS running HBS 3 (Hybrid Backup Sync.) Tracked as CVE-2021-28799, if exploited, this vulnerability allows remote attackers to log in to a device. This vulnerability was exploited by a

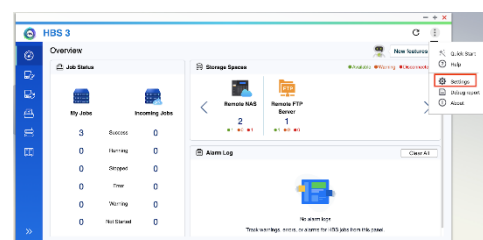


Image source: <https://www.qnap.com/>

ransomware known as Qlocker, attacked the QNAP NAS running certain versions of HBS 3 (Hybrid Backup Sync). To prevent infection from Qlocker ransomware, it is recommended updating the HBS 3 to the latest version. CVE-2021-28799 has CVSS score of 10.0 by QNAP.

Multiple Vulnerabilities in Mesa Labs' AmegaView

Source: <https://us-cert.cisa.gov/ics/advisories/icsa-21-147-03>

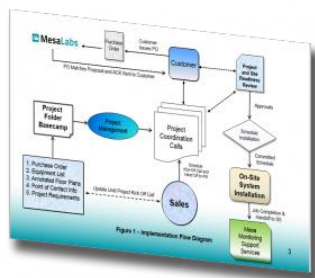


Image source:

<https://monitoring.mesalabs.com/>

Multiple Vulnerabilities were identified in Mesa Labs' AmegaView. CVE-2021-27447 and CVE-2021-27449 are critical Command Injection vulnerabilities having CVSS score 10 and 9.9 respectively. CVE-2021-27445, having CVSS score 7.8, is an Improper Privilege Management vulnerability. CVE-2021-27451 is an Improper Authentication having CVSS score 7.3. CVE-2021-27453 is an Authentication Bypass Using an Alternate Path or Channel vulnerability with CVSS score 7.3. Successful exploitation of these vulnerabilities could allow remote code execution or allow access to the device.

Critical Vulnerability in Plone

Source: <https://nvd.nist.gov/vuln/detail/CVE-2021-33509>

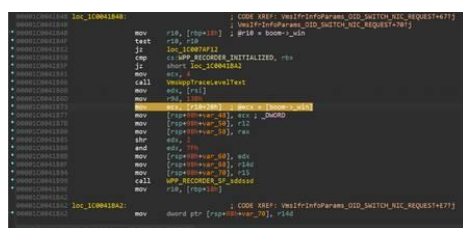


Image source: <https://plone.com/>

Plone is an open-source content management system built on top of the Zope application server. It was discovered that Plone has a critical vulnerability tracked as CVE-2021-33509. This vulnerability allows remote authenticated managers to perform disk I/O via crafted keyword arguments to the ReStructuredText transform in a Python script. CVE-2021-33509 has CVSS score of 9.9.

Remote Code Execution Vulnerability in Hyper-V

Source: <https://msrc.microsoft.com/>, <https://www.theregister.com/>



Proof of concept exploit for crashing a Hyper-V host from the guest

A Remote Code Execution vulnerability has been identified in Hyper-V. Tracked as CVE-2021-28476 has a CVSS score of 9.9. This flaw exists in Hyper-V due to improper input validation. This flaw enables a guest VM to force the Hyper-V host's kernel to read from an arbitrary address. Reading an unmapped address could result in a denial of service of the Hyper-V host. Successful exploitation of this vulnerability could result in complete compromise of a vulnerable system.



Image source:

<https://www.wpbeginner.com/>

Critical Vulnerability in EWWW Image Optimizer

Source: <https://nvd.nist.gov/vuln/detail/CVE-2016-20010>

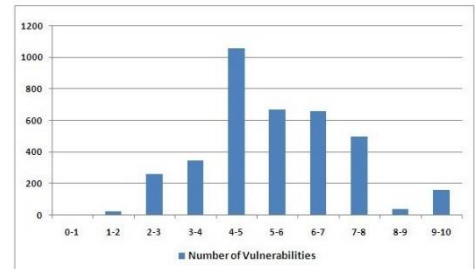
A critical remote code execution vulnerability was identified in the EWWW Image Optimizer plugin. EWWW Image Optimizer allows

remote command execution vulnerability as it relies on a protection mechanism involving boolval, which is unavailable before PHP 5.5. Tracked as CVE-2016-20010 has CVSS score of 10. This flaw affects all EWWW Image Optimizer before version 2.8.5.

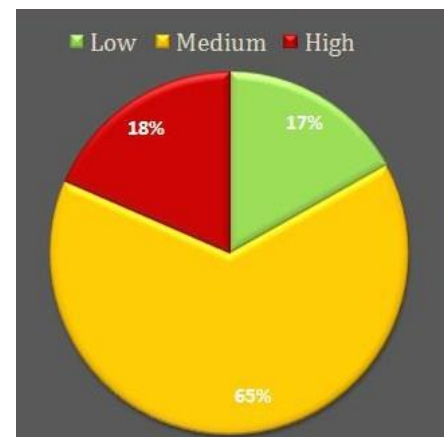
Quarterly Vulnerability Analysis Report

KMS Team, NCIIPC

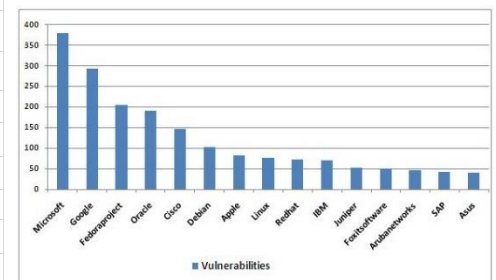
A total of 3679 vulnerabilities have been observed during last quarter, out of which majority of vulnerabilities have score ranging from 4-7. 18 percent of total vulnerabilities reported were of high severity. Microsoft, Google, Fedoraproject, Oracle and Cisco were the top five vendors having 33 percent of total reported vulnerabilities.



Severity	CVSS Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Mar	Apr	May		
Low	0-1	0	0	0	0	622
	1-2	7	14	0	21	
	2-3	68	91	98	257	
	3-4	123	108	113	344	
Medium	4-5	312	449	293	1054	2376
	5-6	195	275	198	668	
	6-7	203	293	158	654	
High	7-8	156	200	137	493	681
	8-9	18	9	6	33	
	9-10	52	57	46	155	
Total		1134	1496	1049		3679



S. No.	Vendor	No. of Vulnerabilities			Total
		Mar	Apr	May	
1.	Microsoft	132	147	101	380
2.	Google	105	80	109	294
3.	Fedoraproject	103	72	31	206
4.	Oracle	2	181	7	190
5.	Cisco	45	43	59	147
6.	Debian	35	55	13	103
7.	Apple	8	74	1	83
8.	Linux	32	20	25	77
9.	Redhat	33	24	15	72
10.	IBM	17	20	33	70
11.	Juniper	0	53	0	53
12.	Foxitsoftware	11	6	34	51
13.	Arubanetworks	27	20	0	47
14.	SAP	21	14	8	43
15.	Asus	1	38	1	40



Security App



RASP highlights critical areas in a vessel's networks and recommends ways to improve and fix the faults quickly.

Rapid Attack Simulation PenTest (RASP)

Source: <https://www.hellenicshippingnews.com/>

A pentest can identify a system's/network's vulnerabilities to attack and estimate how vulnerable those are. An extensive pentest methodology is very much quick and cost effectively assesses the security posture of a vessel even while it is underway. It has been launched by Cyprus based cybersecurity specialist Epsco-Ra security systems known as RASP (Rapid Attack Simulation PenTest). This RASP provides a deep dive into an Information Technology (IT) infrastructure's critical security measures to test and expose deficiencies. RASP highlights critical areas in a vessel's networks and recommends ways to improve and fix the faults quickly. Usually, RASP takes 24 hours to produce full report which includes quantitative scoring, threat matrix, endpoint configuration analysis. Firewall and network assessment as well as malware and command and control simulation. When you execute a RASP, Epsco-Ra Security Systems works with someone onboard and start to test how well your firewall functions and how well it is configured and tests the anti-virus software to see how up to date and functional it is and then they do a vulnerability assessment scan on the bridge network.



Image Source: <https://pbs.twimg.com/>

The Aviary dashboard helps network defenders to analyse PowerShell logs and analyse mailbox logins to determine if the activity is legitimate or not.

Tool to Review Microsoft 365 Post Compromise Activity

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

The Cybersecurity and Infrastructure Security Agency (CISA) released a new tool to accompany the open-source Power shell-based sparrow detection tool released in the month of December 2020 to help network defenders to detect potential compromised accounts in their Microsoft Azure, Microsoft 365 and Office 365 environments. The newly released tool named, Aviary is a Splunk based dashboard that can be used to visualise and analyse data outputs. The Aviary dashboard helps network defenders to analyse PowerShell logs and analyse mailbox logins to determine if the activity is legitimate or not. PowerShell usage by employees can also be monitored along with Microsoft Azure AD domains to determine if they have been modified. To make use the Aviary dashboard, users must ingest Sparrow logs, import Aviary .xml code into the dashboard, point Aviary to Sparrow data using the index and host selection, and review the output.

Healthcare Application Meet Cyber Security Needs

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

The healthcare sector is under constant threat and cyber-attacks

have significantly increased during the COVID-19 pandemic. Cyber criminals are using phishing and ransomware campaigns stealing patient's data, disrupting healthcare services and even putting patient lives at risk. That is why enhancing the security of networks and devices is fundamental to protect the healthcare sector from incidents and threats. The procurement plays a fundamental role in this context by shaping the ICT environment of modern hospitals and ensuring cyber security is taken into consideration at every step. European Union Agency for cyber security (ENISA) has released a web based online tool to help healthcare organisations address cyber security challenges. This implemented tool can be used in the process of identifying standard procurement practices to achieve cyber security objectives when procuring services or products.

European Union Agency for Cyber security (ENISA) has released a web based online tool to help healthcare organisations address cyber security challenges.

Cyber Security Platform for Rail Industry

Source: <https://www.razorsecure.com/>

RazorSecure, a rail cyber security specialist, launched RazorSecure Security Gateway, a platform which acts as cyber security barrier that can be deployed across complex rail networks to minimise the risk of cyber-attacks on rail networks. This newly developed platform has been designed specifically for the unique challenges faced by rail industry and helps train manufactures and operators to implement new measures to assure digital safety across their fleets, including the ability to:

- Separate critical networks and analyse traffic in real time.
- Prevent unauthorised network access
- Ensure all network communications are controlled and permitted.
- Aggregate cyber security data for fleet monitoring in real time.
- Can be configured with a range of various virtual machines to identify, protect, detect and respond to new cyber security risks across rail fleet.
- Maintain a consistent and powerful security profile for the entire life of assets.



RazorSecure, a rail cyber security specialist, launched a platform called RazorSecure Security Gateway which acts as a cyber security barrier that can be deployed across complex rail networks to minimise the risk of cyber-attacks on rail networks.

CISA Builds a Defensive Tool for Security Teams

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

The US Cybersecurity and Infrastructure Security Agency (CISA) released a tool- CISA Hunt and Incident Response Program (CHIRP) which helps in collecting the forensic evidence and indicators of compromise (IoC) from on-premise systems. This tool can satisfy the demand of smaller companies and security teams that want to verify if they have missed a compromise. CHIRP is also

CHIRP is also helpful to organisations that do not have access to in-house resources or commercial tools.

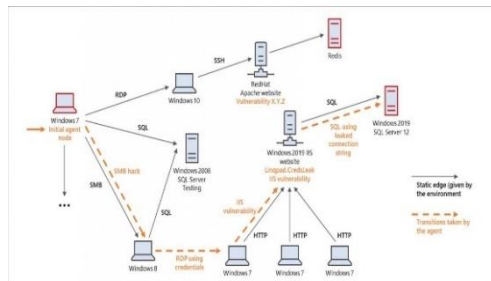
helpful to organisations that do not have access to in-house resources or commercial tools. The CHIRP program also identifies some techniques used by malware to persist in environments, credential exfiltration scripts, and a variety of enumeration and lateral movement techniques.

This tool is designed as an interim mitigation for customers who are unfamiliar with the update or patch process or those who have not yet applied the on-premises Exchange security update.

Microsoft Released One-click Exchange Mitigation Tool

Source: <https://gbhackers.com/one-click-exchange-mitigation-tool/>

Microsoft released a one-click mitigation tool named Microsoft Exchange On-Premises Mitigation Tool (EOMT) to allow customers to immediately address the vulnerabilities exploited in the recent attacks. This tool is designed as an interim mitigation for customers who are unfamiliar with the update or patch process or those who have not yet applied the on-premises Exchange security update. This tool includes the latest Microsoft Safety Scanner with the help of which customers are able to automatically mitigate CVE-2021-26855 on any Exchange server on which it is deployed. This tool is not a replacement for the Exchange security update but this can be used as a fastest and easiest way to mitigate the highest risks to internet-connected, on-premises Exchange Servers before patching.



Demonstration of lateral movement in a network

The simulation environment is configured by a fixed network topology and a predefined set of vulnerabilities that agents can utilise to move laterally in the network.

Microsoft Released Open-Source Cyber Attack Simulator Tool

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

Microsoft has released an open-source AI controlled cyber-attack simulator tool named 'CyberBattleSim' that allows data scientists and researchers to create a simulated environment and see how they fare against AI controlled cyber agents. This 'CyberBattleSim' is an experimentation platform to identify the interactions of automated agents operating in a simulated abstract enterprise network environment. This simulation gives a high-level abstraction of computer networks and cyber security topics. The simulation environment is configured by a fixed network topology and a predefined set of vulnerabilities that agents can utilise to move laterally in the network. The target of the attacker is to take ownership of a portion of the network by exploiting vulnerabilities that are planted in the computer nodes. While the attacker attempts to access the complete network, a defender agent watches the network activity and tries to detect any attack taking place and mitigate the impact on the system by ejecting the attacker. It provides a basic stochastic defender that detects and mitigates ongoing attacks based on predefined probabilities of success. It contains mitigation mechanism by reimaging the infected nodes, a process abstractly modeled as an operation spanning over multiple simulation steps.

MITRE Released D3FEND to Tailor Defences

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

MITRE released D3FEND, a framework for cybersecurity professionals to tailor defences against specific cyber threats, thereby reducing a system's potential attack surface. D3FEND is a technical knowledge base of defensive countermeasures for common offensive techniques. It is complementary to MITRE's ATT&CK, a knowledge base of cyber adversary behaviour. D3FEND establishes terminology of computer network defensive techniques and highlights the previously-unspecified relationships between offensive and defensive techniques. Governments and industry use ATT&CK as a foundation to develop specific cyber threat models and methodologies. Complementary to the threat-based ATT&CK model, D3FEND provides a model of ways to counter common offensive techniques and enumerate how defensive techniques impact an actor's ability to succeed. National Security Agency (NSA) and MITRE encourage the cybersecurity community to promote the adoption of this vocabulary by cybersecurity professionals across government, industry, and academia.

The screenshot shows the MITRE D3FEND framework interface. It features a grid of defensive techniques organized into columns representing different attack phases: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, and Exfiltration. Each column contains a list of specific defensive techniques, such as 'Network Intrusion Detection', 'Endpoint Protection', 'Intrusion Prevention', 'Data Loss Prevention', 'Email Filtering', 'Web Filtering', 'DNS Filtering', 'Firewall', 'Intrusion Detection', 'Endpoint Protection', 'Intrusion Prevention', 'Data Loss Prevention', 'Email Filtering', 'Web Filtering', 'DNS Filtering', 'Firewall', etc. The interface also includes a search bar and a filter button.

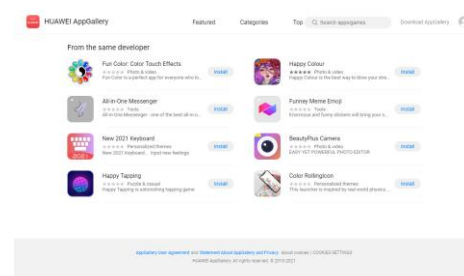
D3FEND establishes terminology of computer network defensive techniques and highlights the previously-unspecified relationships between offensive and defensive techniques.

Mobile Security

Malware Apps in APKPure and Huawei AppGallery

Source: <https://thehackernews.com>, <https://news.drweb.com>

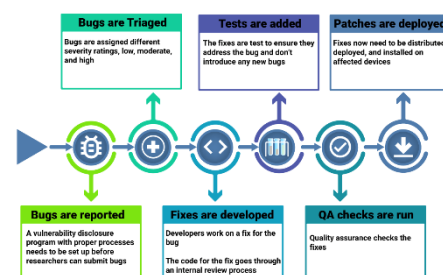
Researchers from Doctor Web and Kaspersky have found out that APKPure v3.17.18 is spreading malware. The version is found to be tweaked to incorporate an advertisement SDK which delivers malware to a victim's device by acting as Trojan dropper. The malware belongs to Android. Triada family which is capable of downloading, installing and uninstalling software without users' permission. The malware can collect device information, open browser tabs, show ads in lock screen and download other malware. Recently, Doctor Web researchers also found out 10 apps in Huawei's AppGallery infected with Joker malware. APKPure has released v3.17.19 on April 9, 2021 after removing the malicious component.



Rust Support for Android Open-Source Project

Source: <https://security.googleblog.com>, <https://thehackernews.com>

Google has been adding Rust support to the Android Open-Source Project for the past 18 months to address memory safety bugs which represents around 70% of Android's high security vulnerabilities. Though managed languages like Java and Kotlin are found to be best for app development and Java is extensively used to effectively protect large portion of Android platform from memory bugs, they do not address the lower layer of the OS. The

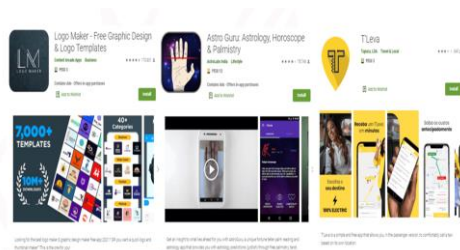


lower layer of OS written in C and C++ requires extensive research in detecting, fixing and mitigating memory safety bugs. On the other hand, Rust programming language uses a combination of compile-time and run-time checks to address the memory safety problem. Currently, Rust is being tested on Android 11 by completely rewriting Android's Bluetooth stack, dubbed Gabeldorsche.

Apps Exposing User Data

Source: <https://blog.checkpoint.com>

Check Point Research (CPR) noticed around 23 android applications in Google Play Store with misconfigured real-time-databases, exposed keys in push notifications and cloud storage keys embedded in apps. The app download ranges from 10,000 to 10 million. These misconfigurations may lead to personal information leakage of users. Astro Guru, a popular astrology app is found to be having misconfigured real-time databases. After analysing, it is found that T'Leva, a popular taxi app, is leaking chat messages between drivers and passengers and also their pick up and drop locations. With the help of leaked cloud storage keys, CPR researchers have found stored recordings of users' device screen in cloud by "Screen Recorder" app. The same vulnerability is also found in "iFax" app leaking documents sent by its users. It is recommended for developers to perform extensive security checks before releasing apps in Google Play Store.



After analysing, it is found that T'Leva, a popular taxi app, is leaking chat messages between drivers and passengers and also their pick up and drop locations.

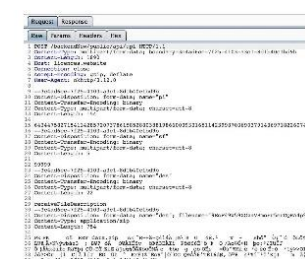


Image source:
<https://www.bleepstatic.com/>

Once the app is downloaded, android device registered with the firebase command and control reports details to attacker.

Fake 'System Update' App Targets Android Users

Source: <https://www.bankinfosecurity.in>

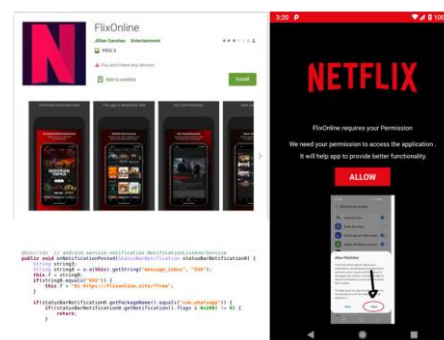
Researchers have spotted a sophisticated spyware app that disguises as system update application in android device. This app can steal data, messages, images and take control of phones. This malicious app function as remote access trojan (RAT) that receives and executes commands to collect and exfiltrate data and perform malicious actions such as stealing messages and database files, inspecting the bookmark, search history of browsers and search for files with specific extension. It can record audio and phone calls, periodically take pictures, monitoring the GPS location. This app is available only in third-party store. Once the app is downloaded, android device registered with the firebase command and control reports details to attacker. App contains update and refreshAllData option. Here update option collects device information and send to C&C whereas refreshAllData option generates a new firebase token. The spyware's functionality and data exfiltration triggered under multiple conditions such as when new contact added, new SMS received or new application installed. The firebase communication is used

to issue commands and dedicated C2 server to collect the stolen data.

WhatsApp-based Wormable Android Malware in Play Store

Source: <https://thehackernews.com/>

A piece Android malware has been discovered which is directly downloadable from the official Google Play Store and capable of propagating via WhatsApp messages. The malicious "FlixOnline" app masquerading as a Netflix app requests intrusive permissions that allow it to create fake Login screens for other apps, with the goal of stealing credentials and obtain access to all notifications received on the device. The application designed to monitor and hide WhatsApp notifications from users and automatically reply with a specially-crafted payload received from the Command & Control (C2) server. After successful infection, the malware is capable of spreading further via malicious links, steal data from users' WhatsApp accounts, propagate malicious messages to users' WhatsApp contacts and groups, and even threaten user to leak sensitive WhatsApp data or conversations. Users should be careful enough to download attachments or links that are received via WhatsApp or other messaging apps, even when it appears to come from trusted contacts or messaging groups.



NCIIPC Initiatives

CSI's webinar on Cyber Security Requirements of National Critical Infrastructure

NCIIPC East zone participated in Webinar on "Cyber Security Requirements of National Critical Infrastructure" organised by Computer Society of India (CSI) on 26th June 2021. Participants from Govt, industries and academia attended the webinar. Various case studies of cyber-attacks in Power & Energy and BFSI sectors were discussed. NCIIPC initiatives like Incident Reporting, Vulnerability Disclosure and Malware Reporting were discussed at length during the event. Several Universities and students showed interest to work with NCIIPC.



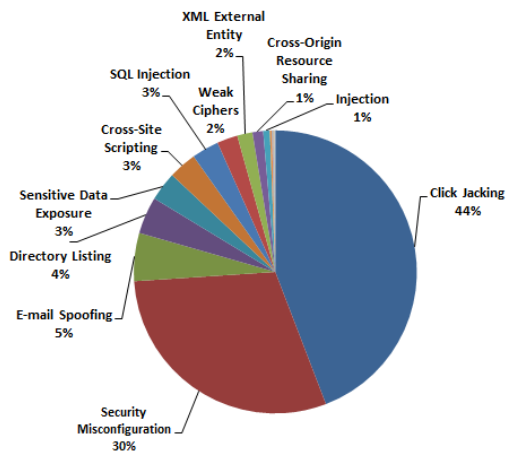
NCIIPC Responsible Vulnerability Disclosure Program

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 2929 vulnerabilities reported during the second quarter of 2021. The top 10 vulnerabilities are:

- Click Jacking





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

Around 338 researchers participated in RVDP programme during the second quarter of 2021. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Arpita Dey
- Ashutosh
- Ashutosh R Mishra
- Bhavak Dipakkumar Kotak
- Bismaya Kumar Panda
- Farhin Malek
- Harinder Singh
- Harshad Pachore
- Pratik
- Pratik Chotaliya
- Sachhit Anasane
- Sachin Mishra
- Samprit Das
- Sanem Sudheendra
- S Rahul

Upcoming Events - Global

July 2021

- 18th International Conference on Security and Cryptography (SECRYPT), Virtual 6-8 Jul
- St. Louis/OKC Cyber Security Summit, Virtual 7 Jul
- 5th International Symposium on Cyber Security Cryptology and Machine Learning (CSCML), Virtual 8-9 Jul
- Blockchain and Internet of Things Conference (BIOTC), Ho Chi Minh City 8-10 Jul
- International Workshop on Cryptography, Security and Privacy (IWCSPP), Budapest 9-11 Jul
- Detroit Cyber Security Summit 2021, Virtual 14-16 Jul
- The 7th International Conference on Artificial Intelligence and Security (ICAIS), Dublin 19-23 Jul
- Black Hat USA 2021, Las Vegas 31 Jul-5 Aug



JULY 2021

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

August 2021

- Techno Security & Digital Forensics Conference Colorado 2021, Denver 2-4 Aug
- SANS Security Awareness Summit & Training 2021 Virtual 3-14 Aug
- ISACA Manila Chapter Webinar: Information Security for Data Privacy, Manila 4-5 Aug
- 30th USENIX Security Symposium, Virtual 11-13 Aug
- 2021 International Conference on Network & Information Security (NISecurity 2021), Stockholm 13-15 Aug
- ISMG Virtual Cybersecurity Summit: Fraud & Payments Security, Virtual 17-18 Aug
- Chicago Virtual Cybersecurity Summit 2021, Virtual 24 Aug
- Cybersecurity Summit Asia: Healthcare, Virtual 24-25 Aug

AUGUST 2021

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

September 2021

- FutureCon San Diego CyberSecurity Conference, Virtual 1 Sep
- INTERFACE Boise 2021, Boise 2 Sep
- Enterprise Security & Risk Management Americas 2021, Virtual 2 Sep
- Arab Security Conference, Cairo 5-7 Sep
- Cyber Security & Cloud Expo Global 2021, London 6-7 Sep



Denver, CO

Techno Security & Digital Forensics Conference

August 2-4, 2021
Hilton Denver City Center





SEPTEMBER 2021

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

OCTOBER 2021

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

- Miami/South Florida Virtual Cybersecurity Summit 2021, Virtual 16 Sep
- ISMG Cybersecurity Summit: Brazil, Virtual 28-29 Sep
- National Cyber Summit (NCS) 2021, Huntsville 28-30 Sep

October 2021

- Cyber Intelligence Asia 2021, Jakarta 5-7 Oct
- Cybersecurity & Fraud Summit: Toronto, Virtual 12-13 Oct
- ElevateIT: Houston Technology Summit 2021, Virtual 13 Oct
- Cybersecurity Summit: Africa, Virtual 13-14 Oct
- Critical Infrastructure Protection & Resilience North America, New Orleans 19-21 Oct
- SAMA PARTNERS Cybersecurity Conference 2021, Mannheim 21-22 Oct
- Texas Cyber Summit, San Antonio 29-30 Oct

Upcoming Events - India

- Gartner Data & Analytics Summit, Virtual 4-5 Aug
- BSides Noida 2021, Virtual 12-13 Aug
- ACCESS'21, Ernakulam 2-4 Sep
- Gartner Security and Risk Management Summit, Mumbai 3-4 Sep
- India CISO Summit 2021, Virtual 9-10 Sep
- Global Digital Security Forum India (GDSF) 2021, Mumbai 16-17 Sep
- NULLCON 2021, Goa 21-25 Sep
- IoT India Expo 2021, Bengaluru 22-24 Sep



General Help

helpdesk1@nciipc.gov.in
helpdesk2@nciipc.gov.in

Incident Reporting

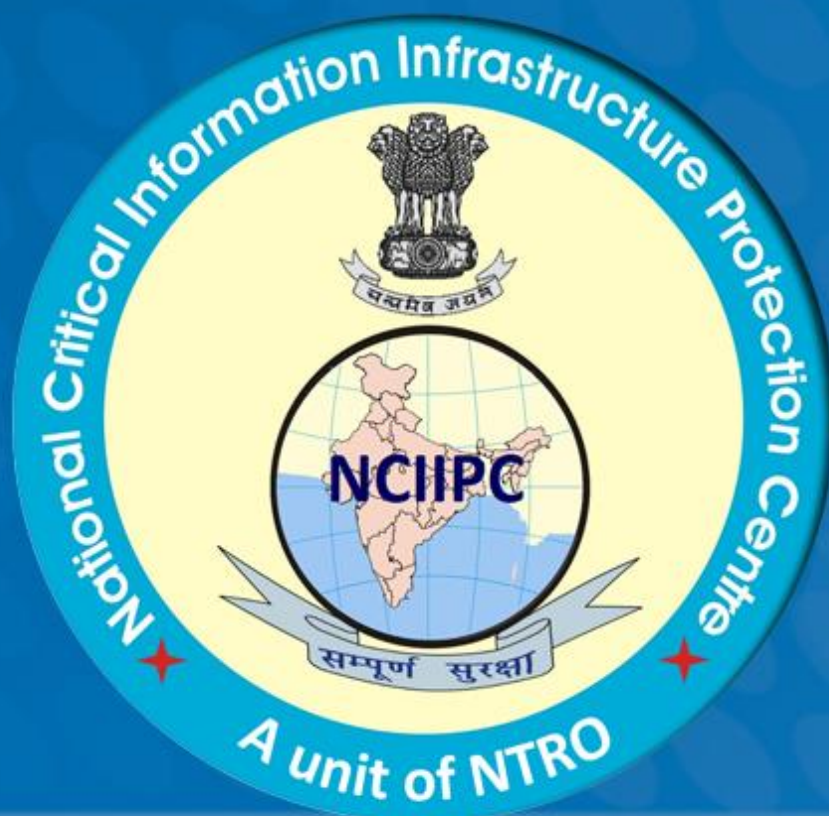
: ir@nciipc.gov.in

Vulnerability Disclosure

: rvd@nciipc.gov.in

Malware Upload

: mal.repository@nciipc.gov.in



Feedback/Contribution

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

Copyright

NCIIPC, Government of India

Disclaimer

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