NEWSLETTER

January 2021

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

SOCIAL ENGINEERING ATTACKS

2
It is impossible to compromise these systems as they follow best security practices

3
May be we can try through the weakest link of Security Chain, i.e., HUMAN !!

Social Engineering Vaccine

Don't click on email attachments from unknown sources

Don't run unknown files with exaggerated titles

Don't install apps from informal sources

"I dream of a Digital India where Cyber Security becomes an integral part of our National Security."

-Hon'ble PM Sh. Narendra Modi

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

VOLUME 5 ISSUE 1

@NCIIPC

NCIIPC Newsletter

January 2021

Inside This Issue

Message from the NCIIPC Desk

NCIIPC will celebrate its 7th Raising Day on 16th January 2021. It was designated as the National Nodal Agency for all measures to protect Nation's Critical Information Infrastructure (CII) under Section 70A of the Information Technology Act 2000 (amended 2008) on that date in 2014.

NCIIPC provides strategic leadership and coherence across government to respond to national level cyber threats against the identified CIIs by developing and executing appropriate national and international co-operation strategies, policies, standards and best practices.

NCIIPC also evaluates niche and innovative technologies relevant to CIIP by working closely with public sector industries, academia and international partners.

Year 2020 witnessed an abnormal increase in cyber-attacks either directly targeting the Health Sector or Social Engineering attacks using Covid-19 themes. 'Work from Home' became a 'New Norm'. While its benefits are undeniable, it also enhanced the attack surface available to the Threat Actors.

Supply Chain Contamination remains a major cause for concern. A number of organisations worldwide have been affected through software updates from OEM. NCIIPC along with other stakeholders are committed to address this challenge and create robust and resilient cyber ecosystem for our nation.

The response to NCIIPC's outreach initiatives has been overwhelming. There was a substantial increase in the number of young and passionate volunteers for NCIIPC Internship Program. Contributions by cyber security researchers in NCIIPC's Responsible Vulnerability Disclosure Program (RVDP) touched a new high. We compliment them for their unwavering commitment towards securing the nation's CII.

NCIIPC wishes its Readers a very Happy and Healthy 2021.

Comments, suggestions and feedback are welcome. You may write to us at newsletter@nciipc.gov.in

News Snippets - National

India 2nd most Targeted Country for Ransomware

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

India ranked second only to the US among the countries, as most impacted by ransomware threats. The most sophisticated & common attack is Double Extortion attack where attacker first extract large quantities of sensitive information prior to encrypting a victim's databases and then will threaten to publish until ransom paid. India has been the worst hit by ransomware in Asia Pacific (APAC) region, with 74 per cent of organisations having suffered a ransomware attack this year. The organisations fast changing towards digitisation have brought cyber security to the cloud in order to keep pace with modern threats and secure organisations 'work from anywhere' operations. Indian organisations feel most threatened by eCrime groups (90%), hacktivists (77%) and insider threats (66%) followed by threats from nation states (64%). The results showed that 76% respondents feel most threatened by cyberattacks originating from China followed by Pakistan (48%) and Russia (43%).

The most sophisticated & common attack is Double Extortion attack where attacker first extract large quantities of sensitive information prior to encrypting a victim's databases and then will threaten to publish until ransom paid.

IRDAI sets Panel for Standard Cyber Liability Insurance Product

Source: https://bfsi.economictimes.indiatimes.com*, https://www.irdai.gov.in*

Amid the COVID 19 pandemic, stimulus rise in incidences of cyberattacks and a growing number of high-profile data breaches caused as the online exposures of offices, business organisations and other establishments continued to increase more globally networked and complex. The Insurance Regulatory and Development Authority of India (IRDAI) has set up a Working Group to explore possibility of a basic standard product structure to provide insurance coverage for individuals and establishments to manage their cyber risks. The General Liability policies do not cover cyber risks and cyber insurance policies currently available are highly customized for clients in a new and quickly growing market. The Working Group will study the lawful provisions on Information and Cyber Security Transactions. The group will examine & recommend possible insurance strategies and scope of the cyber liability insurance covers. The group will also explore possible standard coverages, exclusion & extension for various categories.

The IRDAI has set up a Working Group to explore possibility of a basic standard product structure to provide insurance cover for individuals and establishments to manage their cyber risks.

Indian Railway to Build Cybersecurity Team

Source: https://www.deccanherald.com/

The Indian Railways has begun identifying officers with technical aptitude and upskill them in cyber security in order to subdue online breaches. Certain strength of officials from each Railway Unit with aptitude in ICT software, hardware, networking and

compliances are to be identified for forming the group for that Unit. These officials will be trained in both theoretical and practical aspects of cyber security through a course prepared by MeitY. This unit would work under the supervision of the nominated CISO of the Railway Unit.

43 Mobile Apps Banned by Government of India

Source: https://www.pib.gov.in/PressReleasePage.aspx?PRID=1675335

An order under section 69A of the Information Technology Act was issued by Ministry of Electronics and Information Technology (MEITY) dated 24 Oct 2020 to block the 43 Mobile Apps to protect the interests of citizens and sovereignty & integrity of India. Indian Cyber Crime Coordination Centre, Ministry of Home Affairs found these Mobile Apps involvement in malicious activities against India in their comprehensive report.

News Snippets - International

CISA says Threat Actor Breached Federal Agency's Network

Source: https://www.securityweek.com/, https://us-cert.cisa.gov/

The US Federal Agency was compromised by a malicious cyber actor. The threat actors initially leveraged compromised credentials for Microsoft Office 365 accounts, domain administrator accounts, and credentials for the agency's Pulse Secure VPN server using CVE-2019-11510 by sending a specially crafted URI to perform an arbitrary file reading vulnerability. The attackers attempted to view and download help desk email attachments with "Intranet access" and "VPN passwords". The attackers enumerated the Active Directory and Group Policy key and changed a registry key for the Group Policy. In order to establish persistence and Command and Control on the federal agency's network, the attackers created a persistent Secure Socket Shell (SSH) tunnel/reverse SOCKS proxy. The intruders also connected a hard drive in the agency's network they controlled as a locally mounted remote share. The mounted file share allowed the actor to freely move during its operations while leaving fewer artifacts for forensic analysis. The attacker created a local account on the network that allowed to run PowerShell commands and to exfiltrate data stored in compressed Zip files. The malware installed on the network of the federal agency was able to overcome the agency's anti-malware protection.

In order to establish persistence and Command and Control on the federal agency network, the attackers created a persistent Secure Socket Shell (SSH) tunnel/reverse SOCKS proxy.

The UN Maritime Agency Suffered Cyber Attack

Source: https://latesthackingnews.com/

The United Nations International Maritime Organization (IMO) suffered a cyber-attack on September 30 2020. The attack

affected the website and web-based services, overcoming the robust security measures in place. It took the agency two days to finally pull the website back online on October 2, 2020. The systems and services affected by cyber-attack were Global Integrated Shipping Information Systems (GISIS) database, document repository IMODOCS, and its Virtual Publications service. IMO got ISO/IEC 27001:2013 certification in 2015 for its information security management system.

FBI and CISA Joint Alert for US Government Networks Hack

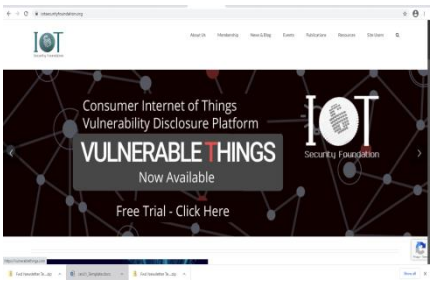
Source: https://securityaffairs.co/, https://us-cert.cisa.gov/

A joint security advisory published by US agencies Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) revealed that Russia-linked APT groups have targeted dozens of the State, Local, Tribal, and Territorial (SLTT) government and aviation networks. The attempted intrusions at several SLTT organisations, successfully compromised network infrastructure on October 1, 2020, and exfiltrated data from at least two servers. The lateral traversal at victim's network allow attacker to access the documents related to sensitive network configurations and passwords, standard operating procedures, IT instructions, such as password resets, vendors and purchasing information & printing access badges etc. The threat actors used the vulnerabilities of multiple products such as Citrix, Microsoft Exchange Servers, Exim versions 4.87–4.91, FortiOS & Windows Servers.

IoT Vulnerability Disclosure Platform Launched

Source: https://www.securitymagazine.com/

The IoT Security Foundation's (IoTSF) VulnerableThings.com online platform has been designed to help IoT Vendors to comply new consumer IoT security standard and regulations. The IoT Vendor will receive, assess, manage and mitigate the risks related to vulnerabilities reported by platform. Many governments in the world such as United Kingdom, Australia, Singapore, Finland and America have already published codes of practice, product labeling schemes or prepared legislation aligned to the standard. This platform will guide manufacturers with policy templates and prompts to resolve consumer IoT vulnerabilities and comply with industry standards. Without the coordinated vulnerability platform, the security of IoT products is diminishing and the risk of attacks are increasing.



The IoT Vendor will receive, assess, manage and mitigate vulnerabilities reported by platform.

Hackers Stole US Government Source Code via SonarQube

Source: www.bleepingcomputer.com, https://beta.documentcloud.org

Hackers exploiting vulnerable SonarQube servers stole data from

U.S. government agencies and enterprise organisations. The threat actor gained access to data source code repositories owned by both government and corporate entities via internet-exposed and insecure SonarQube instances, later exfiltrating it and leaking it publicly. The Federal Bureau of Investigation (FBI) issued a flash alert warning. The SonarQube platform uses 27 programming languages to automate-code for quality auditing and static analysis to discover bugs and security vulnerabilities.

Ransomware Attack on Top Brazilian Court Encrypts Files, Backups

Source: https://www.hackread.com/

A massive ransomware attack happened on 02 & 03 Nov 2020 at official website of Brazilian Superior Court of Justice. The services including the official website were forced to go offline. The entire data was encrypted & all attempts to decrypt the files went vain. In ransom note attacker demanded ransom to decrypt data and given Protonmail based email address for further communication.

The US Senate approved IoT Cybersecurity Improvement Act

Source: https://threatpost.com/

The US Senate has approved an IoT Cybersecurity Improvement Act. This act will improve existing standards and best practices for procuring and managing IoT devices. The act will regulate vendors and buyers to adopt & manage standards-based coordinated vulnerability disclosure processes. This act will ensure strict guidelines for the minimum security of IoT devices.

Trends

Google App Engine Feature Abused to Create Phishing Pages

Image source: https://flicsdb.com/

Source: https://www.bleepingcomputer.com/, https://en.secnews.gr/

A newly discovered technique by a researcher shows how Google's App Engine domains can be abused to deliver phishing and malware while remaining undetected by leading enterprise security products. The problem with Google App Engine is mainly with how subdomains are created. In most cases, cloud services are used by fraudsters to create a malicious application, where a subdomain is assigned. Later, they stay there phishing pages or use the malicious application as a command-and-control server to deliver malware payload. When it comes to Google App Engine, the domain appspot.com Google, which hosts applications, has the following structure: VERSION-dot-SERVICE-dot-PROJECT_ID.REGION_ID.r.appspot.com. In this case, a subdomain does not represent just one application, but represents the version of the application, the project ID and the

region ID fields. However, if any of these fields are incorrect, the name service, the Google App Engine will not display a "404 Not Found" page. Instead, it displays the "default" page of the application. This process is called soft routing. This means that there are variations of subdomains that leads a user to malicious attackers.

The problem with Google App Engine is mainly with how subdomains are created.

Microsoft Uses Trademark Law to Disrupt Trickbot Botnet

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

Microsoft Corporation has implemented a coordinated legal sneak attack in a bid to disrupt the infrastructure used by malware-as-a-service botnet Trickbot. However, it appeared that the operation did not completely disable the botnet. The researchers of both Intel 471 and CrowdStrike reported that the TrickBot operations resumed after a short while. Emotet was observed serving TrickBot payloads to infected machines. Later, it was observed by Intel 471 that Emotet distributed TrickBot samples that include new control servers in their configuration, but these servers were not able to respond to bot requests. Also, according to CrowdStrike, approximately 10,000 bots were seen becoming unreachable after being served a non-standard configuration file. Researchers of Intel 471 reported that the disruption operations against Trickbot are now global in nature and had success against Trickbot infrastructure.

Image source: https://zdnet4.cbsistatic.com/

Microsoft Corporation has implemented a coordinated legal sneak attack in a bid to disrupt the infrastructure used by malware-as-a-service botnet Trickbot.

FBI Warns of Recently Registered Domains Spoofing its Sites

Source: https://www.bleepingcomputer.com/, https://www.ic3.gov/

The U.S. Federal Bureau of Investigation (FBI) has observed that nation/ state-backed or financially motivated threat actors are using phishing domains for gathering victims' credentials, financial information & to spread malware, as well as to propagate false information. The spoofed domains have been created using misspelled versions of legitimate domains such as .com or .net instead of the .gov used by the FBI's official U.S. government website. The FBI's Internet Crime Complaint Center (IC3) issued warning to general public about phishing domains and suggested recommendation:

- The spelling of websites, web addresses & email addresses must be verified.
- Update Operating System, Anti-virus & Anti-malware regularly.
- Should not communicate with unsolicited Email senders.
- Do not share personal data on unsolicited communication.
- Use whitelisting domain with strong two-factor authentication.
- The Secure Sockets Layer (SSL) certificate of visiting websites must be verified.

Identified Spoofed Domains		
agenciafbi.ga	fbiigovv.com	infofbi-unit.com
authefbi.ga	fbi-intel.com	johnsonfbi.com
cyber-crime-fbi.org	fbikids.com	legalienfbi.com
fbi.camera	fbimaryland.org	plapper-fbi.com
fbi.cash	fbimaxwell.com	powerfulfbi.ninja
fbi.ca	fbimostwanted.info	us-fbigov.com
fbi.health	fbi-news.com	virtualfbi.com
fbi.studio	fbinews.ga	xalienfbi.com
fbi.systems	fbinews.online	x-alienfbi.com
fbi.xn--mgbayh7gpa	fbinigeria.org	fbi-fraud.com
fbi0.com	fbi-ny.com	fbidefense.com
fbibau.us	fbioffice.ml	fbienglish.com
fbi2.com	fbi-official.com	fbifrauddepartment.org
fbi-unit.net	fbiofficial.online	fbifraud.primebnkonline.com
fbi3262.live	fbione.com	fbiglobalgp.com
fbi7.cn	fbiopenthedoor.icu	fbigov.art
fbi9.com	fbiorganisation.online	fbi-gov.network
fbi9.me	fbiorganization.club	fbigrantinvestigation.com
fbiagent.online	fbipedophilerings.com	fbiinspectionunit.com
fbi-augustyn.pl	fbiphoto.com	fbi-police.com
fbiaustralia.com	fbireserveco.biz	fbi-c-d.com.co
fbibau.de	fbireport.us	fbicyberdivision.com
fbi-bau.de	fbiusagov.online	hdqkfbi.cn
fbi-biz.com	fbiurl.com	ic-fbi.org
fbiboston.xn--mgbayh7gpa	fbiusagov.com	fbiwarning.club
fbi-c.com.co	fbiusgov.com	fbi-cd.com.co
Registered Spoofed Domains but Currently Unable to Resolve		
fbihelp.org	fbi-belote.com	fbilibrary.ml
fbigiftshop.shop	fbispassport.gq	fbi-pay.com
fbiboston.com.jo	fbi99.cn	fbi2000.com
fbiusa.net	fbi.com.jo	fbipublicidad.com
fbi-usa.us	fbi058.com	

Image source: https://images.digitalguardian.com/

This initiative is an attempt to organize the different techniques employed by malicious adversaries in subverting ML systems.

New Framework released to Protect Machine Learning Systems

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

Microsoft released a new open framework called Adversarial ML Threat Matrix in collaboration with IBM, MITRE, NVIDIA, and Bosch to help security analysts to detect, respond, and remediate adversarial attacks against Machine Learning (ML) systems. This initiative is an attempt to organise the different techniques employed by malicious adversaries in subverting ML systems. The threat matrix is the result of partnership among 12 industry and academic research groups with goal of empowering security analysts to orient themselves to these new and upcoming threats. The threat matrix framework is seeded with a curated set of vulnerabilities and adversary behaviours that Microsoft and MITRE have vetted to be effective against production ML systems.

Phish Scale Trains Employees to Avoid Phishing

Source: https://www.helpnetsecurity.com/

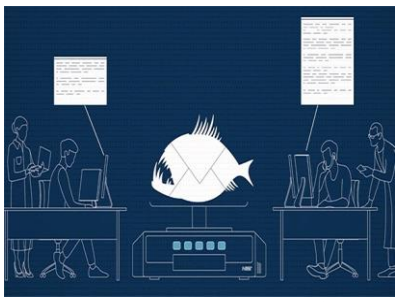


Image source: https://www.nist.gov/

The Phish Scale uses a rating system that is based on the message content in a phishing email.

The National Institute of Standards and Technology (NIST) researchers have developed a new method called Phish Scale that could help organisations train their employees to avoid phishing, The Phish Scale provides a deeper understanding of whether a specific phishing email is easier or harder for a particular target audience to detect. The Phish Scale uses a rating system that is based on the message content in a phishing email. It uses five elements that are rated on a 5-point scale that relate to the scenario's premise. The overall score is then used by the phishing trainer to help analyse their data and rank the phishing exercise as low, medium or high difficulty. The idea behind Phish Scale is to give CISOs a better understanding of their click-rate data instead of relying on the numbers alone. There can be several reasons behind a low click rate for a particular phishing email: either the phishing training emails are too easy or do not provide relevant context to the user, or the phishing email is similar to a previous exercise. Such data can create a false sense of security if click rates are analysed on without understanding the phishing email's difficulty.

Mozilla Boosts Security in Firefox with HTTPS-Only Mode

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

Mozilla has released Firefox 83 with a new improved security feature known as HTTPS-Only Mode. The HTTPS-Only Mode is designed to prevent eavesdropping on websites containing sensitive information like medical details, emails, or financial data. With HTTPS-Only Mode enabled, Firefox attempts to establish a fully secure connection for each and every site the user accesses, and also asks for user's permission before connecting to a site that lacks support for secure connections. Mozilla expects that

the usage of HTTP connections to be reduced once HTTPS is more widely supported.

'MDBR' Service Blocks Connections to Malicious Domains

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

The Malicious Domain Blocking and Reporting (MDBR) service has been formed by partnership between the U.S. Cybersecurity Infrastructure Security Agency (CISA), Centre for Internet Security (CIS), and Akamai Technologies. The MDBR service adds another layer of DNS security to help protect applications of organisation. It prevents connections to harmful domains, MDBR technology aims to reduce infections through known ransomware, malware, phishing and other cyber-threats. Organisations can take advantage of MDBR by simply pointing their DNS requests to DNS servers of Akamai. Then all DNS lookups are proactively compared against a list of known and suspected malicious domains. Attempts to connect to these domains are blocked and logged, and CIS' security analysts provide members with reports on these blocked requests, in addition to helping with remediation, if needed. Organisations are also provided with specific reporting and CIS deliver regular reporting and intelligence services to its members.

It prevents connections to harmful domains, MDBR technology aims to reduce infections through known ransomware, malware, phishing and other cyber-threats.

NAT Slipstreaming Hack Tricks Firewalls and Routers

Source: https://portswigger.net/

The NAT Slipstreaming is a JavaScript-based attack, which allows an attacker to remotely access any TCP/UDP service bound to a victim's machine, bypassing victim's Network Address Translation (NAT) or firewall security controls. A victim is first tricked into visiting a site under the hacker's control. The NAT Slipstream attack works across all major modern browsers by taking advantage of arbitrary control of the data portion of some TCP and UDP packets without reference to HTTP or other headers. NAT Slipstreaming exploits a flaw in how some routers and firewalls implement Application-Level Gateway that allows NAT to be bypassed.

NAT Slipstreaming exploits a flaw in how some routers and firewalls implement Application-Level Gateway that allows NAT to be bypassed.

Cybercriminals use Spyware to Access COVID-19 Research Data

Source: https://threatpost.com/

Many mobile phishing attacks are targeting pharmaceutical companies. After breakout of the COVID-19 pandemic, they have shifted their focus from credential theft to malware delivery. As pharmaceutical companies race to develop COVID-19 vaccine, mobile phishing groups are upgrading their tactics in hope to acquire critical researches. Previously cybercriminals targeted pharmaceutical company employee's credentials. New

As pharmaceutical companies race to develop vaccine for COVID-19, mobile phishing groups are upgrading their tactics in hopes to acquire critical researches.

research shows that in third-quarter of 2020 77 percent of pharmaceutical mobile phishing attempts delivered malware on victims' systems. This shift, which reflects a 106 percent increase in malware delivery in mobile phishing, shows cybercriminals turning to spyware, remote access functionality and more in order to access the COVID-19 research data from pharmaceutical companies.

Sneaky Office 365 Phishing Inverts Images to Evade Detection

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

According to WMC Global analysts a creative Office 365 phishing campaign is inverting images used as backgrounds for landing pages to avoid getting flagged as malicious by crawlers designed to spot phishing sites. These inverted backgrounds are often used as part of phishing kits that attempt to duplicate legitimate login pages as closely as possible to collect target's credentials by tricking them into entering them into a fraud login form. The tricky part that makes this detection evasion method feasible is that a potential victim would notice the inverted image instantly and become suspicious and leave the site immediately. To avoid this, the phishing kit automatically revert the backgrounds using Cascading Style Sheets (CSS) to make them look just like the original backgrounds of the Office 365 login pages they are trying to mimic. The targets that get redirected to one of these phishing landing pages will see the original background instead of the inverted image backgrounds that the web crawlers will be served with.

Original version next to inverted background (PhishFeed)

The tricky part that makes this detection evasion method feasible is that a potential victim would notice the inverted image instantly and become suspicious and leave the site immediately.

Cyber Storm 2020

Source: https://www.cisa.gov/cyber-storm-2020

Cyber Storm is a cyber exercise held by U.S. Cybersecurity and Infrastructure Security Agency (CISA). It brings the public and private sector together to simulate response to a cyber crisis impacting the critical infrastructure. The main goal of Cyber Storm 2020 is to strengthen cybersecurity preparedness and response capabilities by exercising policies, procedures, and processes, in order to identify and respond to a multi-sector cyberattack targeting critical infrastructure. The Cyber Storm 2020's objectives include:

- Examining the implementation and effectiveness of national cybersecurity plans and policies.
- Strengthening and enhancing information sharing and coordination techniques used across the cyber ecosystem during a cyber incident.
- Reinforcing public and private partnerships and enhance

their potential to share timely and relevant information.

- Implement communications aspects of cyber incident response to refine and mature communications strategies.

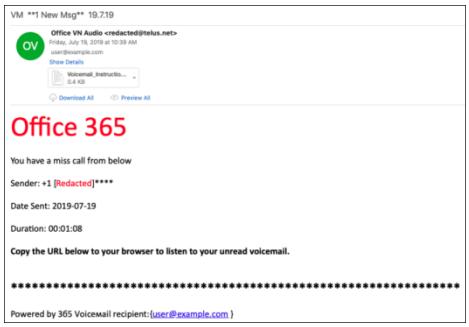
The Cyber Storm 2020 was aimed at:

- Build upon the outcomes of previous exercises and changes to the cybersecurity landscape.
- Evaluate and upgrade the capabilities of the cyber response community.
- Promote public-private partnerships and strengthen relationships.
- Integrate new critical infrastructure partners.

The main goal of Cyber Storm 2020 is to strengthen cybersecurity preparedness and response capabilities by exercising policies, procedures, and processes, in order to identify and respond to a multi-sector cyberattack targeting critical infrastructure.

Google Services Weaponized to Bypass Security in Phishing

Source: https://threatpost.com/

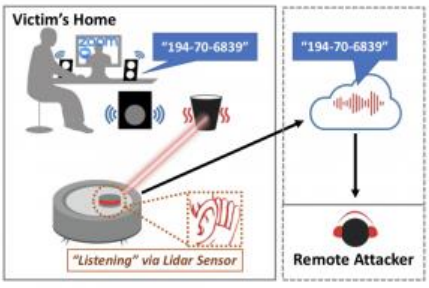


Arjun Sambamoorthy, a cyber security researcher has published a report on how services like Google Docs, Google Forms and others are being misused by malicious actors in order to give their spoofing attempts a false facade of legitimacy, both to victims and security filters. One campaign used a Google Form and an American Express logo to lure victims to enter sensitive information. Firebase, Google's mobile platform, was also used to host a phishing page that allowed it to sneak through email filters for Firebase being trusted. In another attack, an email was delivered to victims asking them to assess a secure message on Microsoft Teams. The link led to web page with a forged Office 365 login portal hosted on Google Sites. Mobile Gmail users have been targeted by sophisticated cyberattack through fraudulent, unsolicited meeting notifications. Google faces a fundamental dilemma because what makes their services free and easy to use also lets cybercriminals build and launch effective phishing attacks. The ability for malicious actors to leverage Google Services for their activities is emerging as a trend.

Google faces a fundamental dilemma because what makes their services free and easy to use also lets cybercriminals build and launch effective phishing attacks.

Robot Vacuums Suck Up Sensitive Audio in 'LidarPhone' Hack

Source: https://threatpost.com/



Researchers have uncovered an attack that allows attackers to eavesdrop on homeowners inside their homes, through the LiDAR (Light Detection and Ranging) sensors on their robot vacuums. The attack, called "LidarPhone" by researchers, targets vacuums equipped with LiDAR sensors. LiDAR is a remote sensing method that uses light in form of a pulsed laser to measure distances to and from nearby objects. The technology helps vacuums navigate around obstacles on the floor while they clean. The good news is that the attack is complex. Attackers would need to

The attack, called "LidarPhone" by researchers, targets vacuums equipped with LiDAR sensors.

have already compromise the device itself. Additionally, attackers would need to be on the victim's local network to launch the attack. Regardless, the attack serves as an important reminder that the proliferation of smart sensing devices in our homes opens up many opportunities for acoustic side-channel attacks on private conversations.

BFSI Segment needs to Build-up its Cyber Security Infrastructure

BFSI Sector, NCIIPC

The Indian BFSI segment has been one of the rapidly growing segments within the country, fueled by fast paced technology adoptions and supportive Government policies. The Industrial 4.0 revolution, that integrates smart technology enabled tools with day-to-day business operations, leveraging AI, ML, and cloud computing etc., making vital functions accessible at the touch of wise smart screen. These innovations, integrated with an infinite rise in fin-tech, are helping create a cashless economy for India. However, with the increased digitalization, the increase in cases of cyber security breaches, have exposed several vulnerabilities in the BFSI's ICT infrastructure and operations. Globally, the BFSI Sector has been witnessing an increase in cyber-attacks where skilled hackers are ready to perform purposeful breaches, heists, invasions, data thefts through malware and phishing attacks, resulting in major financial loss and distress. Some important alternate delivery platforms and associated support functions are highly vulnerable and need regular cyber-security posture assessment and trigger necessary corrective/preventive actions to mitigate the identified risks. Following are some of the major areas:

Some important alternate delivery platforms and associated support functions are highly vulnerable and need regular cyber-security posture assessment and trigger necessary corrective/preventive actions to mitigate the identified risks.

App-based Solutions by Fin-tech Start-ups: Over the past few years, a spread of technology start-ups specializing in financial segment have emerged, disrupting the way we make purchases. From app-based wallets and UPI linked instant transactions to single window e-commerce apps, fin-tech start-ups must be mindful of all kind of vulnerabilities and the emerging threats and must invest in creating a sturdy data security framework for the apps. The approach of "Security by Design" has to be followed. This should never be ignored by any boot strapped start-ups to avoid hefty investment as they are also a contributor towards building digitally secure financial ecosystem. The start-ups should collaborate with cyber security firms that provide adapted and value driven services or advisory in the same space. All third-party apps or plug-ins should mandatorily undergo security audits by competent authorities.

Mobile Apps and Integration: As per a report by Avaya India, 26% of Indian customers regularly avail digital banking services

through the bank's web portal and mobile app. With the increased usage of smart phones and also the patron friendly mobile app version for one tap transactions, digital banking is becoming more susceptible to cyber-attacks. Banks should strictly adhere to the regulatory cyber security mandates of RBI and pay special attention to ensure information security.

ATM Security: These are quite common and involve mixture of physical breach – where finger prints and card details are stolen by imprinting the contact point of the machine, and software breaches. As per a report by Positive Technologies, up to 69% of all ATM's are at risk of cyber-attacks. Interestingly, ATM attacks have gotten complex and more sophisticated since the primary ATM Malware attack of 2018, and it's expected to continue being a looming threat. ATM security evaluation, a significant exercise, can be a recommended mode of addressing the emerging threats. Global standards and good practices w.r.t card based & ATM transactions (e.g. PCI-DSS) should be followed. The India Government has released ATM Security Guidelines and mandates through sector regulators.

As per a report by Positive Technologies, up to 69% of all ATM's are at risk of cyber-attacks. Interestingly, ATM attacks have gotten complex and more sophisticated since the primary ATM Malware attack of 2018, and it's expected to continue being a looming threat.

While all of the above are important steps to be taken by BFSI players, including banks, service providers, fintech players and their technical support staff, one of the most significant aspect of secure transactions is consumer awareness.

References:

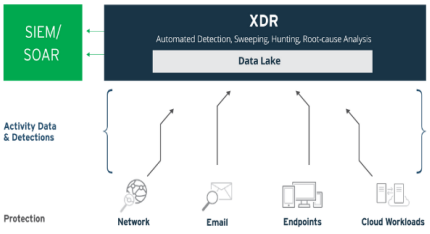
[1] https://www.expresscomputer.in/guest-blogs/why-the-bfsi-segment-needs-to-beef-up-its-cyber-security-infrastructure/64781/

[2] https://www.esds.co.in/blog/cybersecurity-in-the-bfsi-sector-has-stepped-up-get-to-know-why/

Extended Detection and Response (XDR)

Threat Assessment Team, NCIIPC

In View of quick detection and response in Cyber world, it has become necessary to tackle, deploy and defend the cyber-attack during peace as well as during War. Many nations are now maintaining DBMS as their arsenal with respect to various types of attacks through XDR.



- XDR stands for cross-layered detection and response. XDR is a new approach and a key element of defending an organisation's infrastructure and data from damage and misuse.

- XDR automatically collects and correlates metadata from multiple sources like emails, endpoints, servers, cloud

workloads and networks.

XDR extends the range of EDR (Endpoint detection and response) to enclose more deployed security solutions whereas EDR used for malware detection over antivirus capabilities.

- XDR extends the range of EDR (Endpoint detection and response) to enclose more deployed security solutions whereas EDR used for malware detection over antivirus capabilities.
- It utilizes the updated technologies to provide higher detection for capturing threat Intel.
- Threats detection carried out at faster pace so that security analysts can investigate, analyse and identify the threat and respond without delay.
- The events and visibility of threat have to be addressed at higher level. Further it will enable the security teams to eliminate any impact and reduce the severity and scope of the attack.

References:

[1] https://www.paloaltonetworks.com/cyberpedia/what-is-xdr

[2] https://www.cisco.com/c/en/us/products/security/what-is-xdr.html

Domain Fronting Vs Domain Hiding

Director, NSAC, NCIIPC

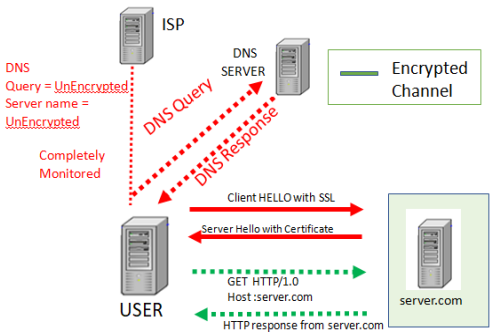


Figure-1

Domain fronting is the technique or mechanism by which actual domain of interest resides behind the primary front domain. Concept primarily got popularized by CDNs (Content Delivery Networks) which is network of Data Centres (DC) distributed across the globe for delivering content with high performance and availability. Domain fronting provided the leverage to the CDNs for blocking the single blacklisted domain without blacklisting the entire IP hosting several other domains, blocking of which may result in collateral damage. There are primarily three areas where domain request while traversing from client to server gets highlighted viz. DNS (Domain Name System) query, TLS SNI (Server Name Indication) and HTTP Host Header. However, Domain Hiding is TLS 1.3 with ESNI (Encrypted Server Name Indication) where the SNI is encrypted, hiding the requested domain.

Data flow: Domain fronting and hiding- As per the basics of HTTP request, user request the domain via DNS query which forms unencrypted channel as highlighted in Figure-1. Even If server is HTTPS enabled, usage of SSL/TLS between client and server includes passing of the respective "client hello" and "server hello" request in clear text. However subsequent request are encrypted

as the encrypted tunnel is formed between client and server. But if the server is not HTTPS enabled, even the subsequent encrypted requests as highlighted in figure1 are also unencrypted subjected to prying eyes of all the stakeholders including ISPs, CDNs, etc.

Genesis of Technology: In year 2003 concept of SNI (Server Name Information) was introduced enabling mapping of multiple domains on to single IP. Accordingly, HTTP/1.1 was introduced as web server with HTTP/1.0 was able to serve only one web portal per IP address due to absence of hostname provision as available in the updated protocol. Accordingly, with HTTP/1.1 there is a provision of Host header resulting in "named virtual hosts". These technological changes helped the CDNs in hosting the desired services with high bandwidth on shared infrastructure. CDN web services enable hosting of multiple domains on single IP behind fronted server. In Domain fronting front domain and the actual domain to be approached must be hosted by the same CDN. In April 2018 domain fronting was stopped by major service providers. Domain fronting works at the application layer with different domain requests at different layer of communication with domain request outside the encrypted request as mentioned:

- DNS request
- TLS SNI
- Inside the encrypted traffic as HTTP Host Header.

DOH or DOT will prevent unencrypted flow and ESNI aims to prevent clear text flow of SNI information in TLS versions TLS1.3 onwards which will even bypass the lens of "nosy" ISP. Domain fronting 2.0/Domain Hiding with release of TLS1.3 will use ESNI (Encrypted SNI), making the entire communication between client and server encrypted as highlighted in Figure-2.

Conclusion: As every technological evolution presents mix picture of their relative pros and cons similarly, Domain Fronting and Domain Hiding have their own merits and demerits. Domain fronting as highlighted in previous paragraphs provides efficient services for delivering the content by serving the request through geographically advantaged servers; however, this technology is also exploited by malicious attackers. As per FireEye APT29 used the mentioned technique for creating the stealthy backdoor in the victim's environment. This APT used the The Onion Router (TOR) with domain fronting plug-in "meek" for creating encrypted hidden network tunnel appears to be connecting to Google as a front domain. Though Domain Hiding is capable of maintaining the privacy through encryption of SNI, however with the advent of domain fronting 2.0/domain hiding where SNI is replaced with ESNI under TLS 1.3 coupled with DoH (RFC 8484); emergence of more sophisticated attacks can be witnessed in due course of time.

CDN web services enable hosting of multiple domains on single IP behind fronted server. In Domain fronting front domain and the actual domain to be approached must be hosted by the same CDN.

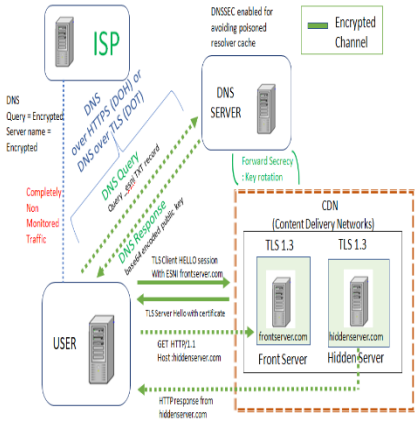


Figure-2

As per FireEye APT29 used the The Onion Router (TOR) with domain fronting plug-in "meek" for creating encrypted hidden network tunnel appears to be connecting to Google as a front domain.

Domain Hiding is capable of maintaining the privacy through encryption of SNI; as with advent of domain fronting 2.0/domain hiding SNI is replaced with ESNI under TLS 1.3.

References:

[1] https;//www.blackhat.com

[2] https://www.defcon.org

[3] https://www.sans.org

[4] https://www.mitre.org

[5] https://resources.infosecinstitute.com

[6] https://www.soc-cmm.com

[7] https://www.ida.org

[8] https://www.researchgate.net

[9] https://www.techbeacon.com

[10] https://www.universalreview.org

[11] https://www.researchgate.net

[12] https://blog.apnic.net

[13] https://www.icann.org

[14] https://www.towardsdatascience.com

[15] https://www.securityintelligence.com

ICT Supply Chain Risk Management Task Force

Telecom Sector, NCIIPC

ICT Supply Chain

A supply chain is a network between industry or organisation and its suppliers to provide and distribute a specific product to end-users. The network includes different activities, entities, information, and resources. Satellite connectivity to financial transactions, thousands of businesses, organisations, and governments depend upon ICT to store information on, interact with, and deliver services to end-users. Well-funded attacks by malicious actors threaten government or industry similar by way of their contractors, sub-contractors, suppliers at the all level of supply chain. Threat actors exploit vulnerabilities within the Information and Communications Technology (ICT) supply chain to achieve access and steal sensitive information along with chain. The ICT Supply Chain Risk Management (SCRM) Task Force is sponsored by CISA's National Risk Management Centre (NRMC). It is the United States' public-private supply chain risk management partnership. The SCRMs main aim is to identify and

develop consensus strategies that enhance ICT supply chain security.

Main task of ICT SCRM Task Force Members: The ICT SCRM Task Force consists of members from large and small private sector organisations (Information Technology, Communications Sectors and Federal Agencies). The main responsibilities of ICT SCRM task members are as below:

The ICT SCRM Task Force consists of members from large and small private sector organizations (Information Technology, Communications Sectors and Federal Agencies).

- It is recommended to develop a common framework for the bi-directional sharing of SCRM threat information between industry and government.
- It is recommended to produce policy for incentivize the purchase of ICT from original manufacturers or authorised resellers.
- It is recommended to develop a SCRM assurance template for vendors.
- It is recommended to Identify processes and criteria for threat-based evaluation of ICT supplies, products, and services

References:

[1] https://www.cisa.gov/ict-scrm-task-force

[2] https://www.cisa.gov/supply-chain

Malware Bytes

DoD, DHS Warn of Attacks Involving SLOTHFULMEDIA Malware

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

U.S. government's malware analysis report includes technical details about a malware named as SLOTHFULMEDIA. It is a dropper that deploys two files when executed. It consists of a RAT which allows hackers to control compromised devices and other component is a dropper that removes dropper, once RAT completely obtains control over targeted computer. RAT is capable of running OS commands, terminating process, taking screenshots, modifying registry and making changes to files. The malware has been used by threat actors against entities in India, Russia, Ukraine, Malaysia. Basically, it is a C++ based backdoor which comes in EXE or DLL variants. It was distributed through spear-phishing emails containing malicious word documents. It uses wsdlpull open-source library to communicate with C2 servers. During research it has been found that SLOTHFULMEDIA is related to PowerPool.

RAT is capable of running OS commands, terminating process, taking screenshots, modifying registry and making changes to files.

PhantomGhost spreads KashmirBlack using DevOps

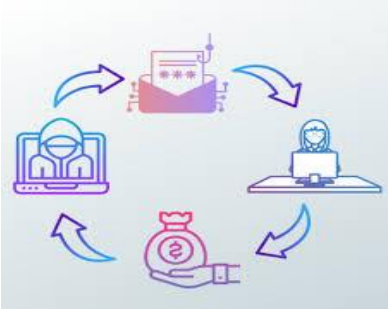
Source: https://www.infosecurity-magazine.com

To drive agility and adding new payloads and exploits, botnet infrastructure is using DevOps techniques.

Researchers have found a highly sophisticated global botnet operation dubbed as 'KashmirBlack'. This botnet has compromised thousands of machines controlled by a single command and control server. Mechanism used by botnet is decade-old PHPUnit RCE vulnerability in Content Management System. This RCE vulnerability allows remote attackers to execute arbitrary PHP code via HTTP POST data beginning with a substring. In most cases, this vulnerability is exploitable when */vendor* folder is publicly accessible. To drive agility and adding new payloads and exploits, botnet infrastructure is using DevOps techniques. It means botnet can rapidly change their repositories as well as their C&C infrastructure to hide its tracks. It is extremely polished operation making use of the recent software approaches. Security vendor has claimed cybercrime group PhantomGhost linked to this botnet.

Seedworm Deploys new Downloader against Mideast Targets

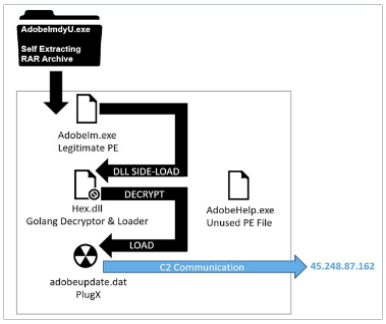
Source: https://www.darkreading.com/



Seedworm an Iran based group has been mainly focused on east-based government organisations. Recently, this group has developed new tools and techniques such as custom download utility known as PowGoop and commodity ransomware as part of their campaign for companies and government agencies. These software downloads and decrypts obfuscated PowerShell scripts to run on compromised systems. Beside this, they have also deployed ransomware named Thanos. These custom tools are for compromising targets and extending their infiltration into networks. PowGoop uses multiple layers of encoded PowerShell scripts to effectively download and execute PS-based payloads. These type of custom tool sets are common tactics used by attacker to confuse attribution and to slow down incident response.

Chinese Threat Actor 'Mustang Panda' Updates Tools

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



A Chinese threat actor tracked as 'Mustang Panda' also referred as TA416 and RedDelta has been known for targeting entities connected to the diplomatic relations between Vatican and the Chinese Communist Party. Threat actor have updated their toolset by including new variant of Golang PlugX malware loader. Hackers used RAR archives that serves as PlugX malware droppers. It includes an encrypted PlugX payload, a legitimate Adobe executable for side loading and a golang binary to decrypt and load the payload. In the past, it has been observed including Google Drive and DropBox URLs within phishing email to deliver

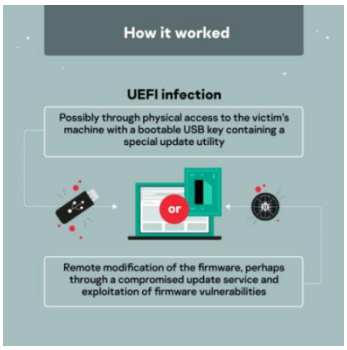
malware and related components. The encrypted PlugX payloads has been disguised as data and gif files along with hardcoded XOR decryption key. The C&C IP for this malware has been hosted by Chinese Internet Service Provider.

It includes an encrypted PlugX payload, a legitimate Adobe executable for side loading and a golang binary to decrypt and load the payload.

Hacking Group used Rare UEFI Bootkit for Espionage

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

A rare UEFI bootkit known as "MosaicRegressor" has been used to target non-government organisations and diplomatic missions with an espionage campaign. UEFI, shorthand for Unified Extensible Firmware Interface helps in initiating the booting sequence within a PC and loads the operating system. The "MosaicRegressor" attempts to take over the device's booting process and downloads multiple malware variants with data-gathering capabilities. It is a multistage and modular framework having four key components. It includes two DXE drivers, which are part of device's firmware and two UEFI applications. This act as dropper that allows the hacking group to load additional malware. All these components are derived from VectorEDK source code. Attackers can modify the firmware to deploy its malicious code that will run after the operating system is loaded. Attack vector for this bootkit needs physical access to targeted PC to load the bootkit using a USB key.

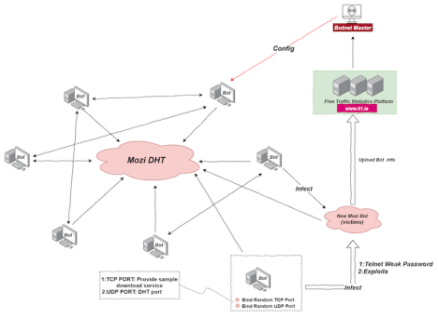


The "MosaicRegressor" attempts to take over the device's booting process and downloads multiple malware variants with data-gathering capabilities.

Mozi Botnet accounted for majority of IoT Traffic

Source: https://www.bankinfosecurity.asia/

Mozi malware has been active since 2019 accounted for 90% of global IoT network traffic. Mozi targets misconfigured IoT botnet with command injection attacks. It is capable of launching distributed denial-of-service attacks as well as delivering spam and other types of malware. It has been found in a variety of devices, including enterprise-grade routers and devices made by Huawei, Netgear and D-Link as well as closed-circuit cameras. It has used peer-to-peer communication protocols to distribute its malware and take control of other device nodes. It also uses brute-force methods from a hardcoded list to bypass weak passwords. Mozi operators use a shell command called wget that helps to gain access and permissions. This command further retrieves a file called mozi.a which executes on the file of the compromised device microprocessors. This enables the operator to install other malware. The mozi botnet also block and bind certain ports, which ensures malware stays on the device. Further, Mozi uses encrypted P2P protocol to look for other vulnerable nodes.

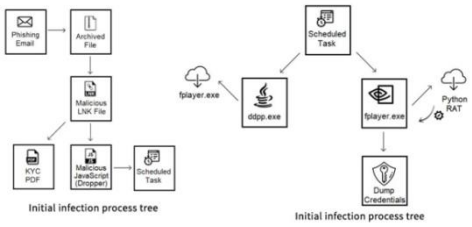


Mozi targets misconfigured IOT botnet with command injection attacks. It is capable of launching distributed denial-of-service attacks as well as delivering spam and other types of malware.

Python-based Spy RAT Emerges to target FinTech

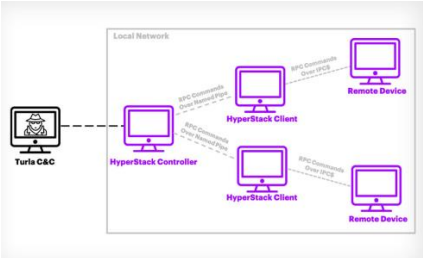
Source: https://threatpost.com/

PyVil, a Python based RAT targeting Fintech companies has been



PyVil provides technique to exfiltrate data, perform keylogging, capture screenshots, run CMD commands, open an SSH shell and install applications such as LaZagne to retrieve passwords stored on a local computer.

developed by Evilnum group. PyVil provides technique to exfiltrate data, perform keylogging, capture screenshots, run commands, open SSH shell and install applications such as LaZagne to retrieve passwords stored on a local computer. Attack vector used by these threat actors, to spread PyVil is spear-phishing emails, which uses Know Your Customer (KYC) regulations to attract its victim. This RAT was compiled using py2exe, a python extension to convert python scripts into .exe. For obfuscation, it uses multiple layers. The first layer of code decodes and decompresses the second layer after that, second layer of python code decodes and loads main RAT and imported libraries into memory. It has been found that for C2 communications it uses POST HTTP requests encrypted with RC4 using hardcoded key encoded with Base64. This Evilnum group emerged in 2018 and since then it has developed various malware. To remain undetected, group is using modified versions of legitimate executables. Thus, email security hygiene is required to be protected from such malware.

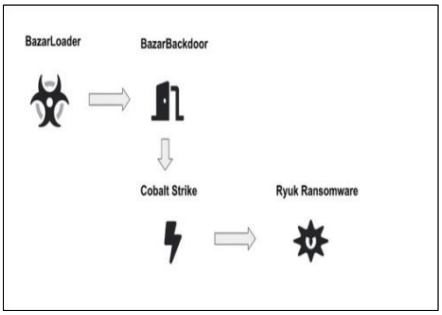


These tools include several layers of obfuscation and defence-evasion technique. It uses various C2 configurations, to allow different re-entry points.

Russian Espionage Group Updates Custom Malware Suite

Source: https://threatpost.com/

Turla, Russia based advanced persistent threat group targets government organisations using custom malware. It has been around for more than a decade. It is known for its malware collection mechanism and interesting command-and-control implementations. It targets government, military and diplomatic targets. Hyperstack a RPC based backdoor and Kazuar, Carbon remote-access trojans identified by researchers. RATs transmit command-execution result and exfiltrate data from the victim's network while RPC based backdoor use RPC protocol to perform lateral movement and issue and receive commands on other machines in the local network. These tools include several layers of obfuscation and defence-evasion technique. It uses various C2 configurations, to allow different re-entry points.



BazarBackdoor attack flow

Ryuk Ransomware Attack

Telecom Sector, NCIIPC

Ryuk is a ransomware that has been targeting Businesses, Hospitals, Government institutions, Enterprises and other popular organizations. It comes under malware family and known for using manual hacking techniques and open-source tools to move laterally through private networks and gain administrative access of all possible computing resources before initiating the file encryption. The attack initiation happens through a phishing e-mail or downloading content by visiting a vulnerable website or clicking on a pop-up. The attack kill chain uses Advanced Persistent Threat (APT) tool to exploit vulnerable machines to install key-logger and steal credentials to create a transparent path to move around the

compromised network. They first look for valuable information to get access then trigger the Ryuk malware to encrypt it. In parallel they keep expanding their footprints in entire network and repeat the same act. Once they get access to the entire system, they send message to the victim for paying ransom for data recovery.

The attack kill chain uses Advanced Persistent Threat (APT) tool to exploit vulnerable machines to install key-logger and steal credentials to create a transparent path to move around the compromised network.

Impact:

- Data loss: organisations or enterprises may have access restriction or loss of important files/ documents upon encryption.
- Financial loss: users are asked to pay ransom in order to decrypt files that were affected.

Recommendations:

- Keep all of your systems and applications up-to-date with latest security patches.
- Create a regular backup and restoration plan and ensure compliance.
- Use Multi-Factor Authentication (MFA) technique for log-in purpose.
- Shutdown unnecessary RDP running on your network.

Recent Incidents:

- The French IT Service Company Sopra Steria hit by a new version of Ryuk ransomware. Due to the ransomware attack, the company has experienced a loss of 50 Million Euros. However, there is no data leakage and no damage to its customers' information systems.
- Another Ryuk ransomware attack happened on Steelcase Inc., one of the largest office furniture manufacturer companies with 13,000 employees. The company detected this ransomware attack on its Information Technology Systems.
- Another instance of attack was on Universal Health Services (UHS), a hospital and healthcare services provider in US and UK. During the attack, multiple antivirus programs were disabled by the Ryuk ransomware and hard drives just lit up with activity. All files within the computers were renamed to .ryk extension. After 1min of this attack, the computers were logged out and shutdown. After they try to power back on the computers, the computers were automatically shut down.

The French IT service company Sopra Steria hit by a new version of Ryuk ransomware. Due to the Ransomware attack, the company has experienced a loss of 50 Million Euros.

References:

[1] www.bleepingcomputer.com/news/security/sopra-steria-expects-50-million-loss-after-ryuk-ransomware-attack/

[2] www.bleepingcomputer.com/news/security/steelcase-furniture-giant-hit-by-ryuk-ransomware-attack/

[3] www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/

[4] www.coresecurity.com/core-labs/articles/what-is-ryuk-ransomware

"Clop" Ransomware Attacked German Tech Firm "Software AG"

Telecom Sector, NCIIPC

The Clop group ransomware is active in attacking organisations across the globe. Recently the Clop group has stolen and encrypted the sensitive information from various organisations and after non-payment of ransom, the stolen information was leaked on their data leak site, hosted on dark web. After encryption CLOP ransomware affixes "Clop" extension in each file and generates a .txt file as "ClopReadMe.txt" containing a ransom note. The Clop ransomware uses the RSA encryption algorithm and keeps keys stored on a hidden server controlled by the Clop threat operators.

Impact:

- Files Encrypted: The Clop Ransomware uses a strong encryption algorithm to make the victim's files inaccessible.
- Financial loss: users are asked to pay the ransom amount in order to decrypt files that were affected.

Recommendations: The best way to protect your data from Clop Ransomware is to have a backup of your files. However, if the computer user has an updated antivirus then the Clop Ransomware can be prevented.

The main goal of Clop ransomware is to encrypt files of an enterprise and asked for payment to provide the decryption key.

Recent Incident: Clop ransomware hit the German tech firm "Software AG" in Oct 2020. Software AG is second-largest software vendor in Germany. Some of the company's most significant customers include Vodafone, DHL, Fujitsu, Airbus and Telefonica. The Clop ransomware group breached the company's internal network and encrypted files on October 3, and demanded more than $20 million for the decryption key. But after negotiations failed, the attacker published screenshots of the company's data on a web site hosted on dark web. The screenshots showed scan copy of employee's passport and ID, employee's email address and financial documents etc.

References:

[1] https://www.cyberswachhtakendra.gov.in/alerts/ClopRansomware.html

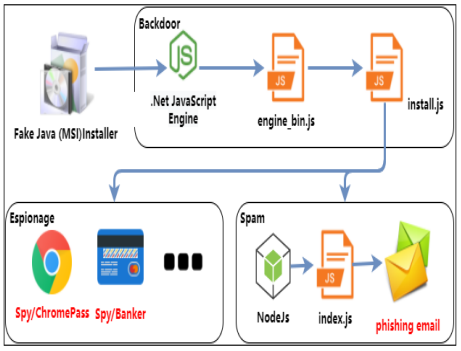
[2] https://threatpost.com/software-ag-data-clop-ransomware/160042/

[3] https://www.zdnet.com/article/german-tech-giant-software-ag-down-after-ransomware-attack/

Secret-stealing Trojan Active releases new Framework SolarSys

BFSI Sector, NCIIPC

To steal the secret or sensitive information, the hacker's communities are widely adopting the new SolarSys distribution framework. SolarSys is mostly active in Brazil which is known for the regions where banking Trojans are highly active. The SolarSys framework is mainly composed of JavaScript backdoors, e-mail worms, and multiple spy modules. The framework uses multiple dynamic domain names mapped with Command &Control server addresses and uses the word-combination Domain Generation Algorithm to generate domain names randomly. When these domains are blocked by the users, the hackers quickly create new domain names to ensure that the overall bot-net does not get affected. SolarSys normally spreads malicious code through fake Windows installers. Once executed, they launch a backdoor in memory that runs the malicious JavaScript which are designed to send phishing emails from the infected PCs. Main motive of this Trojan is to steal information by showing fake online banking login interfaces where people are asked to share their login credentials. Usually, hackers behind this Trojan try to acquire sensitive data that could be misused for making deceptive purchases, transactions, to steal identities, for other spiteful purposes.



The overall workflow

Main motive of this Trojan is to steal information by showing fake online banking login interfaces where people are asked to share their login credentials.

How SolarSys Spreads: Mostly, these Trojans are spread through spam email campaigns. In this campaign, hundreds of malicious emails are sent by criminals that include malicious attachments or contain a website link designed to download perilous files. The moment recipients open, run or execute the attached file, the infection process begins. The attached file are in multiple formats such as Microsoft Office, PDF document, executable file , ZIP, RAR, or JavaScript file.

Recommendations:

- The security patches and service plug-ins should only be downloaded from trustworthy sources and signatures should be verified.
- It is advised not to open files and/or links in such emails without being sure that it has come from an authentic source.
- Additionally, a computer should be scanned with a reputable antivirus or anti-spyware suite regularly.

SolarSys normally spreads malicious code through fake Windows installers.

References:

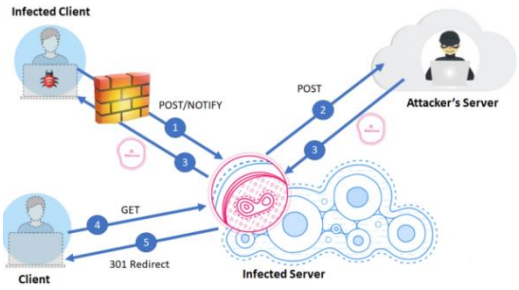
[1] https://cyware.com/news/secret-stealing-trojan-active-in-brazil-releases-the-new-framework-solarsys-ccd68f1f

[2] https://blog.360totalsecurity.com/en/secret-stealing-trojan-active-in-brazil-releases-the-new-framework-solarsys/?web_view=true

[3] https://malware-guide.com/blog/how-to-remove-solarsys-trojan-from-pc

Stantinko's Linux Malware

Transport Sector, NCIIPC



Stantinko's, is one of the oldest malwares that is still operating, and updating its trojan to act as the legitimate "Apache web server" process (httpd) in order to make detection difficult on infected systems. Only the users of Windows were targeted at the beginning, with the malware using infected hosts to show unwanted ads or installing a hidden cryptocurrency miner. As the botnet increased in size and started generating more profits, its code evolved across the years.

Impact: Stantinko malware uses infected hosts to show unwanted ads or for installing a hidden cryptocurrency miner to the victim's system (both Windows & Linux) to carry out brute-force attacks.

Infection Process:

- Stantinko deploy special versions of its malware for Linux systems. Linux version acting as a SOCKS5 proxy, with Stantinko turning infected Linux systems into a larger proxy network.
- Stantinko gang elevate its access to the underlying server OS (Linux or Windows) and then deploys a copy of itself and a crypto-miner to generate more profits for the malware authors.
- The "Stantinko" malware is a modular backdoor, its components implant a loader allowing them to execute any Windows executable sent by the C&C server directly in memory. Well known Stantinko plugins are: Brute-force, Search Parser, Remote Administrator and Facebook Bot.

Stantinko malware uses infected hosts to show unwanted ads or for installing a hidden cryptocurrency miner to the victim's system (both Windows & Linux) to carry out brute-force attacks.

New Stantinko Linux Version: The last version of Stantinko's Linux malware was 1.2. A new version of Stantinko's Linux malware is having a version number of 2.17. The Malware gang might have removed all the chaff from its code and left only the features they desire. It uses the proxy feature for its brute-forcing operations.

Posing as Apache's Web Server: The Stantinko gang appears to have a primer on stealth in this newer release because they have modified the process name its Linux malware uses with httpd, the name usually used by the most famous Apache web server. Linux system administrators need to understand that as the Linux OS becomes more widespread in enterprise environments today.

The Stantinko Malware exploits OS-level vulnerabilities to gain a foothold on a system. This malware gangs usually focus on:

- App misconfigurations that have open ports left or admin panels exposed online.
- Outdated apps left without security patches.

- Systems/apps are using weak passwords for Internet-facing services.
- Tricking the users into taking dangerous actions like social engineering attacks.
- Exploiting bugs in the apps that are running on top of the operating system.

How to Prevent:

- Keep up-to-date malware signatures and engines.
- Conserve operating system patches up-to-date.
- Decrease all the File and Printer sharing services.
- Use robust & Strong passwords.
- Stop the users from installing and operating undesired software applications.
- Execute regular password changes.
- Allow a personal firewall on company workstations that is configured to deny undesirable connection requests.
- Remove unnecessary services on agency workstations and servers.
- Check the users' web browsing habits and restrict access to sites with unsuitable content.
- Practice caution while using removable media.
- Examine all software's downloaded from Internet prior to administering it.
- Manage situational perception of the latest threats and perform the appropriate Access Control Lists (ACLs).

References:

[1] https://www.zdnet.com/article/stantinkos-linux-malware-now-poses-as-an-apache-web-server/

[2] https://securityaffairs.co/wordpress/61250/malware/stantinko-botnet.html

[3] https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/

MODULE NAME	ANALYSIS
Brute-force	Distribution dictionary-based attack on Joomla and WordPress administrative panels.
Search Parser	Performs massive distributed and anonymous searches on Google to find Joomla and WordPress websites. It uses compromised Joomla websites as C&C servers.
Remote Administrator	Backdoor that implements a full-range of actions from reconnaissance to data exfiltration.
Facebook Bot	Bot performing fraud on Facebook. Its capabilities include creating accounts, liking picture or pages, and adding friends.

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

Guest Article

Cyber Threats to CBRN Security

Col Ram Athavale, PhD

Col Ram Athavale, PhD, is a former Key Adviser to the Government of India (MoD and MHA) on CBRN Security.

He has been a Key CBRN Expert for the EU CBRN Risk Mitigation Centres of Excellence initiative in Eastern and Central Africa. A Visiting Faculty at select Indian and overseas universities, a prolific writer and a speaker on CBRN subjects, he has authored a pioneering book titled "Toxic Portents" on 'CBRN Incident Management in India'. Presently he is a freelance CBRN Security and Risk Mitigation Consultant based at Pune, India.

Globalisation, technological advancements and enhanced trade and industry has made our life much easier. While these changes and developments have brought in growth, they have their pitfalls too. Chemical, Biological, Radiological and Nuclear (CBRN) threats are on the rise and the world is becoming a toxic place. CBRN security therefore is of prime concern for most nations today. In fact, it has become a key component of National Security. At the same time, Cyber threats are increasing in their innovative and deadly nature. As many CBRN security systems and analysis devices are based on electronics and use the Internet for data processing, Cyber threats to such security systems are a cause of concern. Imagine hacking of CBRN security systems (like networked detectors and sensors) by Cyber terrorists so as to perpetuate a CBRN attack unhindered.

Vulnerability of CBRN Security Systems: Three prime areas of CBRN security are first: early detection and identification, second: rapid intervention and response and third: protection. Most of these three are interlinked as a continuum. Let us discuss these further.

Trade Tracking: Clandestine trade in CBRN materials has been going on for a long time. In the recent years, thanks to technology, many legitimate shipments are secured by physical as well as electronic means. Geo tagging and RFID of secured orphan sources, critical toxic chemicals or lethal pathogen samples are being widely used today. To add to consignment identification, all shipments are electronically tracked and movement can be monitored from central monitoring stations or by the trading partners. However, all such electronic tracking means are vulnerable to hacking and even alterations. Supply chain breaches and illegal interventions can lead to pilferages and modifications to the contents.

Integrated sensors and detectors: CBRN sensors and detection systems operate on complex electronics and networking. In many cases, especially at critical infrastructure or key military strategic bases, such detectors and sensors are networked with integrated C3I systems and Command Centres. These centres get real time inputs from various deployed CBRN sensors, detectors, meteorological and environmental devices and plot hazards for accurate hazard mapping and prediction of contamination spread. This aids in situational awareness and decision support in the critical moments before or during a CBRN incident or attack.

Advanced systems use cloud-based data sharing for agent confirmation and automated response or counter procedures. Some state-of-the-art systems are AI based to generate optimal reaction protocols and best safety measures. Being primarily

based on electronics and data transfer through wired and wireless (increasingly) networks, these systems need to be secured.

Cyber Threats to Nuclear Power Plants: Cyber threat can raise nuclear risks in two main areas. Firstly, to undermine the security of nuclear materials and facility operations, and secondly to compromise nuclear command and control systems. Hackers could shut down the security system at a nuclear materials storage facility, giving access to terrorists seeking highly enriched uranium, seize control of operations at a nuclear power plant or just steal highly sensitive data from a nuclear facility. Inventory controls, storage mechanisms and processing of nuclear materials, by-products and spent fuel are also areas of cyber security concern. The threat could extend to the command, control, and communications for nuclear weapons.

Automated processes and control mechanisms are susceptible to cyber-attacks and such breaches could cause process malfunctions and release toxic chemicals in the environment.

Chemical Industry and Research Laboratories: Complex electronic security mechanisms at chemical industries using toxic chemicals need to be protected. Automated processes and control mechanisms are susceptible to cyber-attacks and such breaches could cause process malfunctions and release toxic chemicals in the environment. Control mechanisms and inventories at secure warehouses and logistic hubs handling toxic cargo could also be targeted with the aim of pilferage or sabotage. Additionally, high security research laboratories handling sensitive lethal grade chemicals can be breached by cyber-attacks.

Bio Safety Laboratories, Containment facilities and Large Specialty Hospitals: High risk containment facilities and Bio Safety Level (BSL) 3 and above laboratories have complex security mechanisms on site. Such IT controlled security systems are vulnerable to hacks and breaches by cyber terrorists. Similar high-risk areas in multi-specialty hospitals also need to be protected from cyber threats.

Securing CBRN Waste: While most toxic Chemical waste and biomedical waste is destroyed or converted to non-toxic form for further disposal, radioactive waste is a concern and is therefore tagged and stored at secure facilities. In addition, there may be old, forgotten or lost radioactive sources, called 'Orphan' sources that need to be collected, inventoried, tagged and secured. Such security systems use IT enabled devices with networked security programs.

The Solution: It is essential for all critical infrastructures, Nuclear power plants, research laboratories and select Chemical industries to secure their vulnerable IT systems. Especially those that are network based and use Internet-based data sharing and storage. Such facilities need to team up with specialised units including the National Critical Information Infrastructure Protection Centre (NCIIPC), the Computer Emergency Response Team, India (CERT-IN), the National Cyber Coordinator Centre (NCCC) and associated agencies to ensure their vulnerabilities are covered and effectively secured. A concerted National effort by The Ministry of Electronics and Information Technology, to secure CBRN

It is essential for all critical infrastructures, Nuclear power plants, research laboratories and select Chemical industries to secure their vulnerable IT systems.

assets, Chemical Industries, Nuclear power plants and research laboratories is the need of the hour.

Comprehensive Security: Use of wireless technologies for data thefts and introducing viruses and malware have been attempted many times. While Cyber security at CBRN related critical infrastructure is essential, it needs to be seamlessly integrated with physical security measures. Training of technicians and staff on Cyber threats and following physical and cyber security protocols for optimal security is a must. Comprehensive risk analysis and vulnerability assessments are required to plan a wholesome security paradigm for each facility.

Conclusion: CBRN security is a key factor for critical infrastructure. Cyber threats can pose a credible challenge to effective CBRN security. A focused and integrated security protocol with emphasis on Cyber security is essential for CBRN protection. The synergy in these two fields needs to be correctly understood and worked upon by all concerned stakeholders.

CBRN security is a key factor for critical infrastructure. Cyber threats can pose a credible challenge to effective CBRN security.

An approach towards enhancing Mutual Trust Between Critical Infrastructure Organisations and National Cyber Security Agencies

Lt. Col. A J Vijayakumar (Retd), CISSP

Critical Information Infrastructure Organisations comprising of enterprises (both public and private) and Government organizations contribute to the economic development and growth of a nation. Collectively these 'Critical Organisations' create wealth, provide employment to millions of people and bring overall prosperity to the country. There are also a number of government agencies and regulatory organisations that are mandated to protect and monitor the information assets of a nation. These 'Central Agencies' play a vital role in by providing cyber security advisories, best practices, ensuring compliance and assisting in times of cyber emergencies. For this model to be successful, it is essential that these two groups interact in an atmosphere of mutual trust.

Mutual 'Trust Deficit': The Critical Organisations are aware of the cyber security regulations for compliance and the penalties in the event of a security breach. It is likely that there's a tendency amongst such organisations to not report such security breaches to the Government Agencies for apprehension that they may be penalised for non-compliance. Even where security breaches have not happened due to any negligence on the part of the enterprise, due diligence by them can only be demonstrated after a thorough assessment, audit and investigation of a security breach. Such assessment and investigation, is likely to involve substantial time, effort and resources and thereby adversely impact the ongoing business processes and the projects at hand. The process of investigation itself may create an adverse impact on the carefully built 'Brand Reputation'. Hence there's a general apprehension and reluctance to report security breaches on the

Lt. Col. A J Vijayakumar (Retd) has served Tata Communications Ltd. as Chief Information Security Officer (CISO) for nearly 9 years out of his 11 years of service with the company. He is M. Tech. (Computer Science) from IIT Madras.

part of these Critical Organisations. The Government Agencies on the other hand view the Critical Organisations as entities that are more focussed on business outcomes and that they pay less attention to cyber security issues except for mandatory compliance. Experience has shown that this is the common perception existing between both these groups of stakeholders.

The Government Agencies on the other hand view the Critical Organisations as entities that are more focussed on business outcomes and that they pay less attention to cyber security issues except for mandatory compliance.

Challenge of how to enhance this 'Mutual Trust Deficit': Hence It would be a fair assumption to accept that there's a general atmosphere of 'trust deficit' between Central Agencies and organisations in the critical sector. To meet this challenge and bring about enhanced mutual trust, it is suggested that a number of initiatives can be undertaken by the stakeholders such as:

- Enabling Critical Organisations to demonstrate due diligence by regular and close interaction.
- Sharing the updated knowledge base and best practices between and among the stakeholders.
- Assisting the enterprises and enabling them through detailed analysis of vast amounts of cyber security data.
- Reporting cyber security incidents by the Critical Organisations promptly and seeking the assistance of the Central Agencies before a serious security breach occurs.
- Preserving the reputation of the organisations involved in the event of a cyber security event.

Demonstration of due diligence made easier: The Critical Organisations are aware that in the unfortunate event of a security breach, the likelihood of penalties and legal remedies are less harsh if they are able to demonstrate 'Due Diligence' in protecting critical information. Constant interaction with and seeking periodic advisories from the Central Agencies and acting upon them will stand them in good stead in demonstrating due diligence. This would be a good incentive and motivation for the Critical Organisations. This aspect needs to be emphasized in mutual interactions.

Knowledge sharing between the stakeholders can be enhanced through increased interaction between the stakeholders through periodic visits, tele-conferences, seminars/webinars and so on.

Interaction and knowledge sharing between the stakeholders: Knowledge sharing between the stakeholders can be enhanced through increased interaction between the stakeholders through periodic visits, tele-conferences, seminars/webinars and so on. These interactions could cover the mutual sharing of information such as capabilities of the Central Agencies and the challenges and experience of the Critical Organisations. Though this building of 'rapport' takes time, it is found effective. Central Agencies can share the results of detailed analysis of global vulnerabilities, alerts and incident database normally not available with the critical organisations, which will enable the Critical Organisations to enhance their cyber security. On the other hand, sharing of organisation specific challenges faced by the Critical Organisations, would help the Government Agencies to play the role of a 'Threat Analysis Centre' and play a critical role in advising

and evolving best practices as a whole for the Critical Organisations.

Reporting of cyber security incidents: Often, prior to a major security breach at the Critical Organisations, there are enough warning signs in the form of repeated instances of multiple minor security incidents. Many organisations, though concerned, hesitate to approach the Central Agencies for assistance, due to the apprehension that they may be penalised or their reputation may be eroded. It would be a good practice to report the trend of even minor security incidents to Central Agencies, so that prompt action can be taken before a major security breach occurs.

The critical organisations play a vital role in employing large workforce and generating huge revenues for the nation. The central agencies ensure that critical organisations remain protected by advisories, evolving best practices and by enabling better compliance.

Preserving the reputation of the Critical Organisations: On detecting a security breach, most Critical Organisations fear the risk of lowered reputation and tarnished brand image of the enterprise/organisation, at times even more than even the material/financial damage a cyber security incident may cost. It would be a good practice to preserve the confidentiality of the details of the security breach amongst the various government agencies by minimal information sharing and on a 'need-to-know' basis. The Critical Organisations' trust in the Central Agencies will grow manifold when they are confident that their image and reputation will be affected the least.

Conclusion: The Critical Organisations play a vital role in employing large workforce and generating huge revenues for the nation. The Central Agencies ensure that Critical Organisations remain protected by advisories, evolving best practices and by enabling better compliance. Often there's an unspoken deficit of trust between these two sets of organisations, due to which serious cyber security breaches happen which could be avoided if these two stakeholders interact with enhanced mutual trust. This article has suggested some measures to bring about enhanced mutual trust, which would go a long way towards achieving improved cyber security for the nation as a whole.

Learning

NSA issues Cybersecurity Guidance for Remote Workers

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

The U.S. National Security Agency (NSA) has published two cybersecurity information sheets (CSIs) on securing networks and responding to incidents during the period of work-from-home. The first CSI provides details on how teleworkers can identify and mitigate the compromise of their personal networks and to secure data and equipment provided by the government while working remotely. This CSI provides a series of Indicators of Compromise (IoC), along with the mitigation techniques to prevent future compromises. If the IoCs outlined in the document be observed,

users are advised to apply the provided mitigations to any computer, mobile device, or IoT device connected to their personal network. Recommended steps to mitigate the compromise, rebooting and resetting routers, disconnecting infected machines from the network, and removing ransomware infections and restoring a previously backed-up good state. The NSA's second CSI provides information on how to isolate management traffic from operational traffic to system admins for ensuring that a compromised device or malicious traffic does not affect the network operations or compromise the network infrastructure. It provides information on the architecture design of OoB management and recommends to perform vulnerability and risk assessment to decide whether a physically or virtually segmented OoB network architecture is to be implemented. The NSA recommends using encryption protocols and strong encryption algorithms and key sizes, hardening network management devices, managing devices using strong VPNs only, continuously monitoring the network and reviewing logs, and establishing a configuration review and check-in process, which will allow easily identifying malicious changes.

It provides information on the architecture design of OoB management and recommends to perform vulnerability and risk assessment to decide whether a physically or virtually segmented OoB network architecture is to be implemented.

Study on Cyber Incident Response at Electric Utilities

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

The U.S. Federal Energy Regulatory Commission (FERC) and the North American Electricity Reliability Corporation (NERC) have released a report that outlines cyber incident response and recovery best practices for electric utilities. The study found that there is no best Incident Response and Recovery (IRR) plan model. An IRR plan describes how a utility responds to a cyber incident that could operationally and/or financially damage the entity and includes phases and procedures. IRR plans generally define their scope (to whom they apply, what do they cover, and under what circumstances); and define computer security events and incidents, staff roles and responsibilities, levels of authority for response, reporting requirements, requirements and guidelines for external communications and information sharing, and procedures to evaluate performance. The NIST Incident Response Life Cycle identifies the four phases of the incident response process:

- Preparation phase: it is recommended to have a clear definition of personnel roles and empowering staff to take action without any delays, ensuring that employees are professional and are always updating their skills, and incorporating knowledge from past incidents and tests.
- Incident detection and analysis phase: it is recommended to use baselining to detect potential incidents, and using a flowchart or decision tree to quickly assess if a specific risk

An IRR plan describes how a utility responds to a cyber incident that could operationally and/or financially damage the entity and includes phases and procedures.

threshold has been reached.

- Containment and eradication phase: IRR plans must take into account the impact of the steps taken. Another important factor that is needed to be considered in this phase is associated to the resource implications of an incident response of indeterminate length.
- Post-incident activities: it encompasses recovery from an incident and documenting and analysing the incident to prepare lessons-learned reports. Recovery involves restoring the system to an operational state.

Industrial Internet of Things (IIoT)

S&PE Sector, NCIIPC

The Industrial Internet of Things (IIoT) basically an extension of the Internet of Things (IoT) in manufacturing and industrial processes. The main motto behind IIoT is that smart machines are better than humans at capturing and analysing data in real time and they are also better at communicating important information which is used for taking unbiased business decisions faster and more accurately.

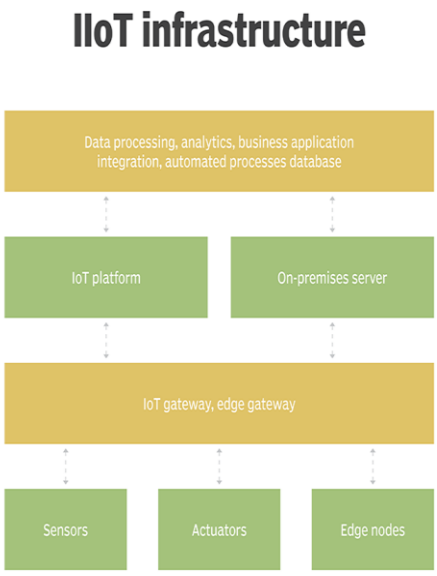


Fig 1: The typical IIoT infrastructure

How IIoT Works: IIoT is a network of smart and intelligent devices which are connected to make systems which can monitor, collect, exchange and analyse data. Each industrial IoT system consists of:

- Intelligent assets that can sense, record and communicate information about themselves
- Data communications infrastructure
- Analytics and applications that converts raw data into business information and
- Human Resources

Smart devices and intelligent assets transmit information to the data communications infrastructure where this raw data/ information is converted into actionable information which can be used for predictive maintenance and execute business processes efficiently.

Industrial IoT systems generally consists of multiple devices, software, hardware, and legacy equipment that weren't designed to work together.

Security considerations and challenges in adopting the IIoT: Since OT devices are being connected to Internet, new challenges will come across which require deep understanding of how IIoT's work. Since IT and OT converge in IIoT systems, cyber security requirements of both the technologies are now absolute necessary. In IIOT, the security requirements extend from virtual to physical environment also. The organisations using IIoT should also consider the risks related to public safety and the impacts posed by cyber-attacks on the communities. There is need to develop strategies that ensure privacy protection and industry related data management regulations. Adoption of international standards and

good practices are also highly recommended. There is also need for protection and management of sensitive information and data. Industrial IoT systems generally consists of multiple devices, software, hardware, and legacy equipment that weren't designed to work together. This brings problems in adoption of new technologies and also has chance for configuration errors, which could compromise the entire system.

Risks to IIoT systems: Security problems and risks arise due to security gaps like exposed ports, obsolete applications inadequate authentication practices and faulty ICT architecture. The convergence of IT and OT introduces real-world threats that could affect even public safety. Unsecure IIoT systems can lead to disruptions in operation and financial losses. More connectivity brings more risks such as software vulnerabilities by which attackers can exploit systems, Internet connected devices and systems that can be searched publicly, malicious activities like hacking, breaches, targeted attacks and system manipulation can cause massive disruptions in business operations. The organisations should not overlook the fact that the OT systems can be compromised through the IT environment like the cyber-attack against a power grid in Ukraine, where the attacker was able to infect the IT infrastructure to shut down critical systems and disrupt power for thousands of households.

Securing the IIoT: Have a security operations centre (SOC). Engage security experts who can understand different kinds of threats so that they can take immediate action in mitigating the effects of attacks. There should be protection in different security layers (device, network and the cloud) of IIoT implementations. Find ways to build security around the legacy systems if they are part of IIoT. Hence, securing IIoT systems requires connected threat defence and end-to-end protection, from the gateway to the endpoint, that should provide:

- Regular monitoring and detection of malware infections.
- Better threat visibility and early detection of abnormal behaviour.
- Prevention of threats and attacks between IT and OT proactively.
- Secure data transfer.
- A next-generation intrusion prevention system (IPS) to prevent attackers from exploiting vulnerabilities.
- Server and application protection across the cloud and the data centre.

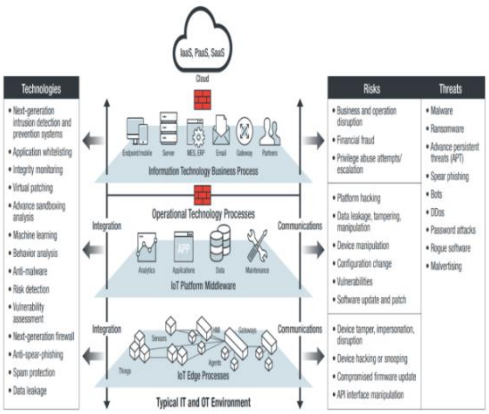


Fig 2: Basic security reference architecture in the new IT/OT environment

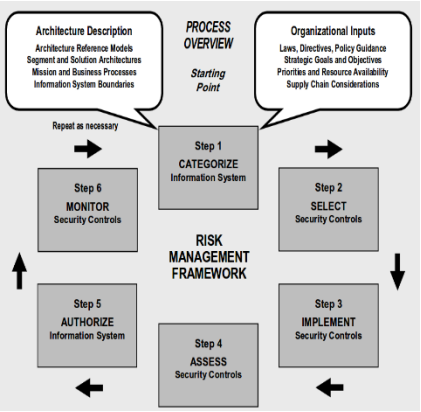
There should be protection in different security layers (device, network and the cloud) of IIoT implementations.

References:

[1] https://www.trendmicro.com/vinfo/in/security/definition/industrial-internet-of-things-iiot

[2] https://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT

[3] https://www.tiempodev.com/blog/industrial-internet-of-things-iiot-cyber-security/



Securing Industrial Control Systems (ICS)

Power and Energy Sector, NCIIPC

Industrial Control System (ICS) is used to operate, monitor and control the industrial processes through different types of control systems and associated instrumentation, which include the devices, systems, networks, automation equipment and controls. Each ICS function is different as per type of industry and are built to electronically manage tasks efficiently. Today, widely available software applications and Internet-based devices have been deployed into most ICS, delivering effective and efficient outcomes, but also increasing system vulnerability.

Vulnerabilities in ICS:

- Communication and network vulnerabilities.
- Software development vulnerabilities.
- Configuration and maintenance vulnerabilities.
- Architecture and design vulnerabilities.
- Policy and procedure vulnerabilities.
- Physical vulnerabilities.

Possible incidents on ICS:

- Disrupted the flow of information through ICS networks, which could disrupt ICS operation Unauthorised changes to instructions, commands, or level 0 device's threshold levels, which could damage, disable, or shut down equipment.
- Inaccurate data sent to workstation operators, to unauthorised changes, or to cause the operators.
- ICS software or configuration settings modification, or ICS software infected with malware, spyware or adware, which could have various negative impacts on operational network. Due to this, Attackers can Interference with the operation of equipment protection systems, Interference with the operation of safety systems.

Disrupted the flow of information through ICS networks, which could disrupt ICS operation Unauthorized changes to instructions, commands, or level 0 device's threshold levels, which could damage, disable, or shut down equipment.

Major security objectives for an ICS implementation:

- Restricting logical access to the ICS network and network activity. Using Data diodes, unidirectional gateways and Demilitarized Zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate networks and ICS networks, and having separate authentication mechanisms and credentials for corporate network users and ICS networks.
- Protecting individual ICS components from exploitation. This includes:
  - Deploying security patches,
  - Disabling all unused ports and services,

  - Restricts ICS user's privileges to authorized person's role;
  - Tracking and monitoring audit trails;
- Using antivirus software and file integrity checking software where technically feasible to prevent, detect, and mitigate malware.
- Detecting security events and incidents: Detecting security events, which can help defenders break the attack chain. This includes the capability to detect disrupted ICS components, inaccessible services, and exhausted resources that are important to provide safe functioning of the ICS.
- Restricting unauthorised modification of data.
- Restricting physical access to the ICS network and devices.
- Restoring the system after an incident.
- Implementing a most secure and reliable network topology for the ICS.

Detecting security events, which can help defenders break the attack chain.

References:

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[2] https://www.nist.gov/industry-impacts/industrial-control-systems-cybersecurity

[3] https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/wp-top-20-cyberattacks.pdf

[4] https://www.dpstele.com/blog/major-scada-hacks.php

[5] https://www.trendmicro.com/vinfo/in/security/definition/industrial-control-system#:~:text=Industrial%20control%20system%20(ICS)%20is,and%2For%20automate%20industrial%20processes

Managing Insider Threats at Financial Institutions

BFSI Sector, NCIIPC

By understanding the types of insider threats that exists, organisations can better defend their networks, customers and employees from risks brought by remote working. Following are the types of Insider Threats:

Accidental Insider Threat: The accidental insider can be in many forms. It could be an innocent employee who clicks on a phishing email, unknowingly helping to spread malicious code around the network. It could be an employee who installs unauthorised software. It may be an employee who uses his date of birth as a password or the one who writes their passkey down on a sticky note under their keyboard. It can even be an unwitting IT staff member that incorrectly applies a security patch, opens a back door to log into the network from home, misconfigures a network component, or forgets to change the default password on a

device, or a person who simply forgets to lock a door.

Malicious Insider Threat: Malicious insiders, on the other hand, are not careless or innocent. They know what they are doing, and they have an objective behind tampering with the network and stealing data. Some may be in a difficult financial crisis or have been tempted by a competitor with a promise of a big payoff or a superior job. Financial institutions and banks are likely targets because that's where the money is. Some people may also just be doing it for the thrill of it.

Remote users that work in isolation are also more likely to fall victim to social engineering attacks because they cannot simply ask their manager/senior whether something is legitimate or not.

Remote Worker Threat: This is a newer category of insider threat. Remote workers have been around for decades, but when the number of employees working from home or remote places increase, so do the risks. In addition to connecting to the company network through a potentially non-secure home or public network, these employees may also be using personal devices that are not configured and secured by IT, further increasing the vulnerabilities. There is also the danger that other people in the home might have access to the device. Remote users that work in isolation are also more likely to fall victim to social engineering attacks because they cannot simply ask their manager/senior whether something is legitimate or not. There are fewer restrictions in a work from home when compared with office environment, which will lead to relaxed attitudes around security. At Security Operations Centre, IT team also faces challenges when it comes to the remote worker. Connections from outside also create more traffic logs and more event data that need to be watched for, at a time when IT resources are already on overload. Attacks can simply get lost in these large No. of event data and logs.

Encrypting data in motion is necessary, which is why SSL and IPSec VPN should be used along with strong authentication when connecting remote users to the network and allowing them to access database.

Managing Insider Threat Risk

- Secure Remote Access Connections: Encrypting data in motion is necessary, which is why SSL and IPSec VPN should be used along with strong authentication when connecting remote users to the network and allowing them to access database. This also has to include analysing encrypted traffic, as VPN tunnels can be just as easily used to transport malware and financial data undetected as it can be for legitimate traffic.
- Encrypt Data at Rest: All classified data, including that of which is stored on employee devices, should also be encrypted. If this is not possible, remote workers should be banned from storing data on these devices.
- Deploy Visibility and Access Control Technology: IT teams need to deploy applications or devices which will help them with visibility of users, devices, and applications on the network so that they can control who and what applications have access. Network Access Control and Zero touch Network

Access are critical solutions should have to be installed.

- Prioritize Endpoint Security: Endpoints are common attack vectors, which also mean they must be regularly checked for vulnerabilities and advanced threats. They must also have advanced security solutions installed, such as endpoint detection and response solutions which offer real-time protection against malware and breaches. These solutions should also be combined with a complete security framework that can automatically detect, respond, and manage incidents, thereby protecting data and reducing system downtime.
- Monitor for Unusual Activity: Install SIEM and SOAR technologies to monitor and alert on abnormal login attempts, large data transfers that cannot be explained, or other unusual behaviour.
- Educate the Remote Workforce: Security policies specific to remote working should be explained to all the employees who is working from home or other remote locations. This includes a focus on the awareness of social engineering attack methods such as phishing, baiting and scare-ware
- Penetration Testing and Audit: Because the stakes are very high, it's important for financial institutions to execute thorough penetration testing and audit from the outside in and the inside out. Complimenting the employee training and phishing awareness, sophisticated penetration testers can attempt to move laterally through systems with admin credentials, exposing vulnerabilities before they can be exploited.
- Apply least privilege controls to applications.
- Apply application white-listing, block unused ports, turn off unused services, monitor network traffic to prevent suspicious activities.

Endpoints are common attack vectors, which also mean they must be regularly checked for vulnerabilities and advanced threats.

Install SIEM and SOAR technologies to monitor and alert on abnormal login attempts, large data transfers that cannot be explained, or other unusual behaviour.

References:

[1] https://bfsi.eletsonline.com/managing-insider-threats-at-financial-institutions-during-remote-work/

[2] https://www.isacybersecurity.com/insider-threats-in-banking/

[3] https://nciipc.gov.in/documents/NCIIPC_COVID19_Guidelines.pdf

Ransomware Attacks in Government Sector

Government Sector, NCIIPC

Governments across the world and in India use Information Technology to provide citizen services. The Digital India Program and enablers like Jandhan-Aadhaar-Mobile Technology (JAM) have significantly raised the attack surface in the Government Sector for ransomware attacks. The attack surface is further expanding as agencies add connected devices in locations such

Ransomware is a particularly powerful weapon against governments, who must provide public services over a wide spectrum of governance functions in cities, municipalities, taluks, districts, state and national levels.

as libraries and government offices and with employees working remotely. Ransomware is a particularly powerful weapon against governments, who must provide public services over a wide spectrum of governance functions in cities, municipalities, taluks, districts, state and national levels.

Views on ransomware/recent Worldwide Ransomware attack analysis: In Feb'20, the IBM X-Force Threat Intelligence Index 2020 was released, according to which there has been an increase in the number of ransomware attacks over the past year, with 13 industries worldwide feeling the effects. For the mentioned report, IBM analysed 70 billion security events per day in more than 130 countries. Data from X-Force IRIS, X-Force Red, IBM Managed Security Services and other information on publicly disclosed data breaches were used for the analysis and generation of the report as mentioned. The main three observations as per the analysis are:

- In 2019 More than 100 government entities in the U.S. were affected by ransomware attacks.
- By exploiting Windows Server Message Block vulnerabilities, Majority of the ransomware attempts (80 percent) were conducted.
- In 2019 Ransomware attacks cost these organisations more than $7.5 million.

The biggest security trend for 2020 has been observed after the increase of COVID-19 related phishing and other attacks targeting remote workers. New York City, for example, has gone from having to protect 80,000 endpoints to around 750,000 endpoints in its threat management since work-from-home edicts took place. Ransomware remains a big threat 2020, SenseCy study says that the ransomware attacks it identified were not all triggered by Windows vulnerabilities. Attackers used vulnerabilities in tools used for remote access into Windows networks.

Ransomware delivery channels/ attack methods: Ransomware is a modern type of malicious malware having power to encrypt all data saved within a victim's computer. Various complex sets of evasion techniques are being employed by ransomware attackers so users will have a tough time knowing that they're being eyed for a ransomware attack. Ransomware creators use to establish attacks through the following listed primary delivery channels:

Through Spam Emails: Ransomware creators are using the Spam email campaign to channel attacks to potential victims. Ransomware creators design spam emails to seem coming from a legitimate email address.

Through Exploit Kits: Exploit kits don't need potential victims unlike malicious emails, to click any email or file attachment for spreading ransomware attacks. By means of a compromised website that have been hacked, exploit kits allow ransomware

creators to infect potential victims. Ransomware creators upload malicious code to the compromised website.

Prevention, Response and Mitigation Strategies: It is very important for Governments to have well designed strategies that prevent attacks on their core and critical governance and citizen services functions and processes. The IT professionals responsible for the information should use multi-pronged approach of end-point, network, server, and backup level detection so as to guard data. It's critical for organisation's detection defence to be everywhere, local and remote for both physical and virtual machines. The utilisation of predictive analytics to see the probability that ransomware is working on a server, workstation, or PC is also foremost most powerful tool to observe attacks. The program can alert administrators if ransomware conditions are discovered. When ransomware is detected, communicated and confirmed, the IT staff should immediately execute previously practiced response and mitigation actions. If one can detect the attack as and when it occurs, one is able to restore the systems from clean backup files.

It is very important for Governments to have well designed strategies that prevent attacks on their core and critical governance and citizen services functions and processes.

Conclusion: Ransomware attacks on government IT systems and networks is on rise in India and globally. There is an urgent need for government entities to proactively work on protecting their core and critical governance and citizen services related functions and processes. NCIIPC has been working closely with the government entities to enhance their cyber resilience and protection against debilitating cyber-attacks. Governments are generally more willing to pay ransom because they cannot afford a paralysis in governance and citizen services. From a cost-benefit analysis perspective the ransom amounts are lower than the cost of recouping lost data and systems. Hence, it is very important that all the governments, both central and state levels, as well as government owned entities should have a dedicated focus on ransomware attacks and mitigate the same without paying any ransom.

There is an urgent need for government entities to proactively work on protecting their core and critical governance and citizen services related functions and processes.

References:

[1] https://www.kratikal.com/blog/the-6-biggest-ransomware-attacks-that-happened-in-india/

[2] https://blog.emsisoft.com/en/36303/ransomware-statistics-for-2020-q1-report/

Container Technology: Vulnerabilities and Countermeasures

Cyber Security Audit Group, NCIIPC

Virtualization technology makes use of software to create an abstraction layer over the physical hardware as it provides efficient use of the physical computer hardware. The hypervisor, a

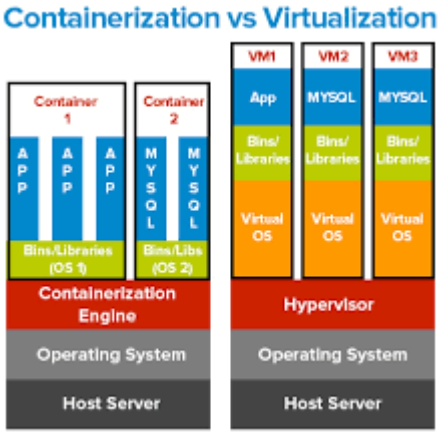


Image Source: https://encrypted-tbn0.gstatic.com/

virtualization software, provides virtual machines (VM), which requires the provisioning of an operating system. These virtual machines isolate applications from each other. Each application is provided with computation, storage and other resources. Provisioning of virtual machines take a lot of time and resources; they don't use system resources efficiently while execution. Containers technology, on the other hand, do not require the provisioning of an operating system. Container applications has its own virtual operating system. This methodology allows better control of resources as containers applications can run completely independent from other container applications running in the container environment. Gartner has predicted that more than 75% of global organisations will be running containerized applications in production by 2022, up from less than 30% in 2020. Container technology has quickly become ubiquitous in the IT industry, with most companies having adopted container technology on some level or contemplating adopting it soon.

Types of Container Technology: Many containerization engines are available. Some of them are open source while the others are commercial ones. Some of the best containerization engines are as Docker, AWS Fargate, Google Kubernetes Engine, Amazon ECS and LXC etc.

Benefits of Container Technology: Containerization enables applications to be deployed quickly. Most of the time, code built in a specific environment when transferred to a new environment, results in bugs and errors. Containerization packages application code and its related configuration files, libraries and dependencies in a single bundle. The resultant container is portable and able to run across any platform or cloud infrastructure.

Use cases of Containers

- Microservices: The process isolation feature makes it easy to break apart and run applications as independent components called microservices.
- Machine learning: Container can be used to quickly scale machine learning models for training and inference and run them close to the data sources on any platform.
- Application migration to the cloud: Container can be used to package entire application and move to the cloud without making any code changes.
- Hybrid applications: It is used to standardize how code is deployed, which makes it easy to build workflows for applications that run between different environments.
- Rapid Development: Containers can reduce the deployment time. Containers can be crated for each process, which can be quickly shared with new applications. While adding or moving a container the Operating system doesn't need to reboot which keeps the deployment time shorter. With shorter

Containers can be crated for each process, which can be quickly shared with new applications. While adding or moving a container the Operating system doesn't need to reboot which keeps the deployment time shorter.

deployment times, we can create and destroy the data created by our containers without any concern.

Major vulnerabilities in Containers: Containers are not built with a security system of their own and thus introduce new attack surfaces that can put the organisation at risk.

Countermeasures for Container Vulnerabilities:

- Containers come from images and developers will either be developing their own images or sourcing them from a third party. So, first thing the SecOps engineers need to look at is the source of the images in their containers. Notary, an open-source Docker project, can be useful in this regard because it allows authors to sign the content they publish and users to verify the authenticity of this content.
- Upgrade vulnerability scanning capabilities to perform scans on container formats. Monitor container runtimes for vulnerabilities.
- Centre for Internet Security (CIS) has published benchmarks for two of the most popular container technologies, Kubernetes and Docker. These CIS benchmarks are the most comprehensive configuration and hardening guidelines for container environments. By removing noncritical native services from the production host, users are forced to access the host through the containers, thereby centralizing control at the container daemon and removing the host from the attack surface.
- A key element in container security is to minimise the number of files stored in particular containers and refresh the containers frequently.
- There are a number of tools available which continually scan for errors in container setup. Docker Bench Security is a CIS benchmarks-based auditing tool that analyses configuration settings for errors.
- Avoid mixing containers associated with sensitive data with containers associated with non-sensitive data.
- Use container-specific host operating systems to reduce attack surfaces.
- Ensure strong authentication and authorisation controls are in place.

CVE	Description	Affected System
CVE-2017-1002101	subPath Volume Mount Vulnerability	Docker
CVE-2017-16995	eBPF Vulnerability	Linux
CVE-2018-1002105	Severe Privilege Escalation Vulnerability	Kubernetes
CVE-2018-8115	Windows Host Compute Service Shim (hcsshim)	Windows
CVE-2018-11757	Docker Skeleton Runtime Vulnerability	Docker
CVE-2018-1000056	Jenkins JUnit Plugin Vulnerability	Jenkins
CVE-2019-1002100	API Server Patch Permission DoS Vulnerability	Kubernetes
CVE-2019-5736	High Severity RunC Vulnerability	Docker
CVE-2019-1003065	Jenkins CloudShare Docker-Machine Plugin Vulnerability	Jenkins

A key element in container security is to minimize the number of files stored in particular containers and refresh the containers frequently.

References:

[1] https://techincidents.com/walkthrough-and-comparison-of-microsoft-container-services/

[2] https://www.gartner.com/en/newsroom/press-releases/2020-06-25-gartner-forecasts-strong-revenue-growth-for-global-co

[3] https://www.cisecurity.org/cis-benchmarks/

[4] https://containerjournal.com/topics/container-security/unpacking-containers-to-find-network-vulnerabilities/

CISA Strategy for 5G Security and Resilience

Telecom Sector, NCIIPC

The US Cybersecurity Agency "CISA" has released a Strategy to ensure the security and resilience of 5G technology for securely deploying 5G network in the United States. The CISA identified 4 lines of effort:

- Simplify domestic 5G Rollout,
- Assess and identify the risks of Core Security principle of 5G Infrastructure,
- Accessing risk of National Economic and Security during Development and Deployment of 5G infrastructure, and
- Global Development and Deployment of 5G should promote.

CISA developed the 5G Strategy. The aim of 5G Strategy is to advance the development and deployment of a secure and resilient 5G infrastructure. It secures national security, data integrity, technology innovation and economic opportunity. Strategy to Secure 5G:

- Support 5G policy
- Expand situational awareness of 5G supply chain
- Partner with stakeholders for strengthen and secure existing infrastructure.
- Encourage for innovation in the 5G marketplace
- Analyse potential 5G use cases and share information on risk management strategies.

The aim of 5G Strategy is to advance the development and deployment of a secure and resilient 5G infrastructure.

References:

[1] https://www.cisa.gov/news/2020/08/24/cisa-releases-5g-strategy-secure-and-resilient-critical-infrastructure

[2] https://www.tripwire.com/state-of-security/security-data-protection/cisa-strategy-5g-infrastructure-security-resilience/

Some important Measures to Prevent Cyber Attacks

Threat Assessment Team, NCIIPC

In view of Covid-19 pandemic, work from home culture is followed in most of the organisations due to which cyber attackers are carrying out cyber-attacks like brute force, ransomware, email spoofing, ICMP Tunneling etc. Given Below are some "Strictly follow" measures to safeguard against these cyber-attacks:

- Carry out vulnerability assessment regularly to check exploitable security loopholes in IT hardware and software infrastructure of organisations.
- Take backup of all sensitive data regularly and keep it separately at secure place.

- Update all machines with latest security patches.
- Employees should not share password at workplace openly they should be encouraged to use unique & strong passwords.
- Make a Sender Policy Framework (SPF), use tools like DMARC, DKIM for your domain, to prevent e-mail spoofing.
- Conduct cyber-attack simulation exercise regularly to assess level of cyber threat awareness among staff and educate them with latest security awareness training tools.
- Always keep file and printer sharing services in disabled mode. If required, use strong passwords enforced through directory service like Active Directory. Do not add users to the local administrator's group unless required.
- Do not open suspicious mail attachments.
- Make sure to scan all software downloaded from the Internet before installing it.
- Enforce security policy on usage of removable storage devices.
- Implement application whitelisting on all endpoint machines. This will reduce droppers or unauthorized software from doing execution & dropping malware.

Conduct cyber-attack simulation exercise regularly to assess level of cyber threat awareness among staff and educate them with latest security awareness training tools.

References:

[1] https://securityboulevard.com

Vulnerability Watch

h2c Smuggling: A new HTTP Request Smuggling

Source https://www.darkreading.com/

Researchers have found a new type of hack in which malicious web requests along with legitimate request could be used to target victims. This new form of HTTP request dubbed as "h2c smuggling". H2c is short form of HTTP/2 initiated by HTTP/1.1 upgrade header. HTTP request smuggling is an exploit in HTTP protocol that uses inconsistency between Content-length and Transfer-encoding headers in an HTTP proxy server chain. This vulnerability has large impact over proxied endpoints. Consumers are not directly affected by this vulnerability but unauthorised access to their data or action take place as the proxied endpoints are affected by this vulnerability. It has been used to access internal management dashboards, IP address spoofing, impersonate actions for other customers or system users and to

HTTP request smuggling is an exploit in HTTP protocol that uses inconsistency between Content-length and Transfer-encoding headers in an HTTP proxy server chain.

take access to the internal network. To stop this vulnerability from being exploited in first place disable websocket support for forwarding upgrade headers.

The threat actor could inject malicious JavaScript payload into any user account even when the registration feature for new patients is disabled.

OpenEMR Fixes Flaws that lead to Command Execution

Source: https://portswigger.net/

A vulnerability has been discovered in OpenEMR instances that could surrender control of the medical practice management application to attackers. Cross-Site Scripting (XSS) flaw in the open-source platform's Patient Portal can lead to unauthenticated command execution on OpenEMR servers. The threat actor could inject malicious JavaScript payload into any user account even when the registration feature for new patients is disabled. These flaws can expose sensitive patient data and critical medical infrastructure. A patch for the vulnerabilities has been released.

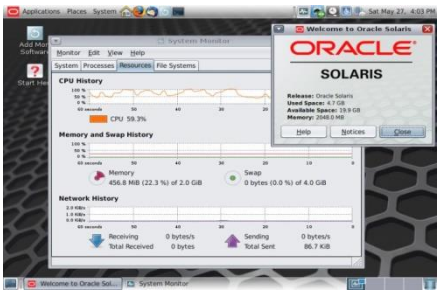
Flaws in PcVue can facilitate Attacks on Industrial Organisations

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

Various potentially serious vulnerabilities have been found in the PcVue SCADA/HMI solution which is developed by France-based ARC Informatique. These vulnerabilities can allow an attacker to execute commands on the computer connected to the OT network and take control of industrial processes or cause disruption. Researchers from Kaspersky has analysed the PcVue product and found three vulnerabilities. The most serious vulnerability which is rated critical and related to unsafe deserialization of messages received in the interface can lead to remote code execution. Other two vulnerabilities have been rated high severity. These vulnerabilities can be leveraged for DoS attacks or information disclosure issue that allows an attacker to access session data of legitimate users. The vendor has patched the security flaws with the release of version 12.0.17.

Sophisticated Threat Actor Exploited Oracle Solaris Zero-Day

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



A zero-day vulnerability has been reported recently in Oracle Solaris operating systems by FireEye. The threat actor has been observed targeting telecommunications companies and leveraging third-party networks to target specific professional and financial consulting industries. The threat actor was observed exploiting a Solaris server that had the SSH service exposed to the Internet. The actor installs the SLAPSTICK backdoor on it, in order to steal credentials. A different Solaris server was observed connecting to the attacker's infrastructure in mid-2020. A remote exploitation tool called EVILSUN to exploit a zero-day impacting a Solaris 9 server is being deployed by threat actor.

SaltStack Reveals New Critical Vulnerabilities

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

VMware-owned company SaltStack has revealed some critical vulnerabilities impacting Salt, an open-source IT infrastructure management solution written in Python. Salt is widely used by data centres worldwide. There are three vulnerabilities that had been discovered. CVE-2020-16846 termed as shell injection in Salt API that was patched by removing the `shell=True` option when calling "subprocess.call" via the SSH client. CVE-2020-25592 is an authentication bypass flaw in Salt API. The patches published for CVE-2020-25592 additionally mentions yet another identifier, CVE-2020-16804. CVE-2020-17490 concerns a permissions issue when opening/saving cryptographic private key files. The fixed releases can be downloaded from PyPI downloads as of now.

CVE-2020-25592 is an authentication bypass flaw in Salt API.

Critical Vulnerability in Google Chrome

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-16011

A critical heap buffer overflow (CVE-2020-16011) vulnerability was discovered in the user interface of Google Chrome on Windows. Successful exploitation may allow a remote attacker to potentially perform sandbox escape via a crafted HTML page. Versions prior to 86.0.4240.183 are affected by this vulnerability. It has a CVSSv3 Score of 10.0.

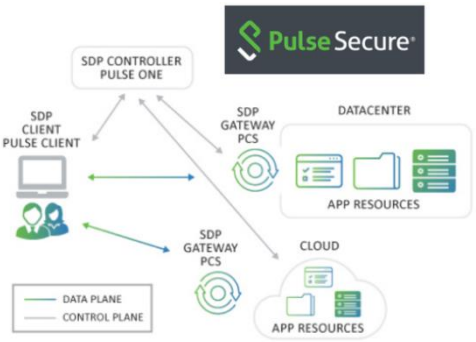
Critical Vulnerability in SAP Solution Manager

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

Multiple Missing Authorisation (CVE-2020-26821, CVE-2020-26822, CVE-2020-26823 & CVE-2020-26824) vulnerabilities were discovered in SAP Solution Manager (JAVA stack). Successful exploitation may allow an unauthenticated attacker to compromise the system because of missing authorisation checks in the SVG Converter Service, Outside Discovery Configuration Service, Upgrade Diagnostics Agent Connection Service and Upgrade Legacy Ports Service respectively. Affected version is 7.20. This has an impact on the integrity and availability of the service. It has a CVSSv3 Score of 10.0.

Vulnerabilities in Pulse Connect Secure & Pulse Policy Secure

Source: https://latesthackingnews.com/, https://kb.pulsesecure.net/



Multiple vulnerabilities such as Improper Authentication (CVE-2020-8206), Code Injection (CVE-2020-8218), Path Traversal (CVE-2020-8221, CVE-2020-8222), Incorrect Default Permissions (CVE-2020-8219), Uncontrolled Resource Consumption (CVE-2020-8220), Exposure of Sensitive Information to an unauthorised actor (CVE-2020-12880, CVE-2020-8216), Cross-site Scripting (CVE-2019-11507,

CVE-2020-8204, CVE-2020-8217), Missing Authorization (CVE-2020-15408) have been discovered in Pulse Connect Secure & Pulse Policy Secure. It is recommended to upgrade Pulse Connect Secure and Pulse Policy Secure server software version to 9.1R8.

The vulnerability exists due to improper inclusion of an open-source file manager library called elFinder.

Zero-Day Vulnerability in File Manager Plugin

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

Critical remote code execution (CVE-2020-25213) vulnerability has been discovered in File Manager (a WordPress plugin with over 700,000 active installations). It has a CVSSv3 score of 9.8. The vulnerability exists due to improper inclusion of an open-source file manager library called elFinder. Successful exploitation may allow an unauthenticated user to execute commands and upload malicious files on a target site. It is recommended to update to the latest version 6.9.

Critical Vulnerability in Yii 2

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-15148

Yii is an open source, object-oriented and component-based MVC PHP web application framework. Critical remote code execution (CVE-2020-15148) vulnerability exists in Yii2 if application calls `unserialize()` on arbitrary user input. It has a CVSSv3 score of 10.0. Versions prior to 2.0.38 are affected by this flaw.

Cisco Warns of Zero-Days in Carrier-Grade Routers

Source: https://www.securityweek.com/, https://tools.cisco.com/

Cisco warned of hackers targeting vulnerabilities (CVE-2020-3566 & CVE-2020-3569) in the Distance Vector Multicast Routing Protocol (DVMRP) feature of IOS XR software that runs on many carrier-grade routers. Successful exploitation may allow an unauthenticated, remote attacker to crash the Internet Group Management Protocol (IGMP) process. All Cisco devices that are running any release of IOS XR software are affected, provided that an active interface is configured under multicast routing and it is receiving DVMRP traffic. OEM has released software updates to address these vulnerabilities.

Critical Vulnerability in SAP Introscope Enterprise Manager

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-6364

SAP Solution Manager and SAP Focused Run allows an attacker to modify a cookie to execute OS commands and potentially gain control over the host running the CA Introscope Enterprise Manager leading to Code Injection. Successful exploitation may allow an attacker to read and modify all system files and also impact system availability. Update has been provided in WILY_INTRO_ENTERPRISE 9.7, 10.1, 10.5, 10.7. The vulnerability has a CVSSv3 score of 10.0.

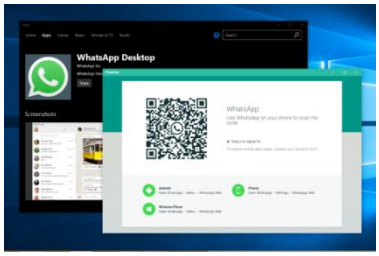
Critical Vulnerability in SonicWall VPN Devices

Source: https://latesthackingnews.com/, https://nvd.nist.gov/

Stack-based buffer overflow (CVE-2020-5135) vulnerability has been discovered in the SSLVPN component of the SonicWall Network Security Appliance. Successful exploitation may allow a remote attacker to cause Denial of Service (DoS) and potentially execute arbitrary code by sending a malicious request to the firewall. It has a CVSSv3 Score of 9.8. Affected products are SonicOS Gen 6 version 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version 7.0.0.0.

Critical Vulnerability in WhatsApp Desktop

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-1889



Improper Privilege Management (CVE-2020-1889) vulnerability has been discovered in WhatsApp Desktop where a security feature bypass issue may allow sandbox escape in Electron and escalation of privilege if combined with remote code execution vulnerability inside the sandboxed renderer process. It has a CVSSv3 score of 10.0. Versions prior to v0.3.4932 are affected by this flaw.

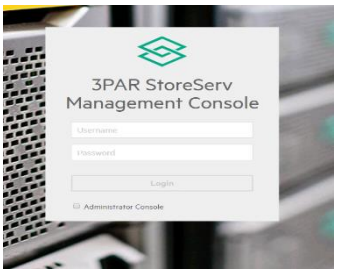
Critical Vulnerability in GitLab

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-13300

An Incorrect Authorisation (CVE-2020-13300) vulnerability has been discovered in GitLab if an OAuth authorisation scope changes without user consent in the middle of the authorisation flow. It has a CVSSv3 score of 10.0. Versions before 13.3.4 are affected by this flaw.

Critical Vulnerability in HPE SSMC

Source: https://securityaffairs.co/, https://nvd.nist.gov/



HPE StoreServ Management Console (SSMC) is a management and reporting console for HPE 3PAR StoreServ systems (AI-powered storage cloud service providers) data center arrays and HPE Primera (data storage for mission-critical apps). Remote authentication bypass (CVE-2020-7197) vulnerability has been discovered in HPE SSMC. Versions prior to 3.7.0.0 are affected by this flaw. The flaw can be exploited by threat actors with no privileges and doesn't require user interaction. It has a CVSSv3 Score of 9.8. HPE has released HPE 3PAR StoreServ Management Console 3.7.1.1 to mitigate the flaw.

The flaw can be exploited by threat actors with no privileges and doesn't require user interaction.

Authentication Bypass Vulnerability in Wireless Router Chipsets

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

Authentication bypass (CVE-2019-18989, CVE-2019-18990, and

CVE-2019-18991) vulnerability has been discovered in chipsets of wireless routers from Qualcomm, Mediatek, and Realtek. Successful exploitation may allow an attacker to arbitrarily send unencrypted packets from a spoofed MAC address and receive encrypted responses. It is recommended that end users with access points that include the identified chipset and firmware versions upgrade or replace vulnerable access points with another access point.

Vulnerabilities in Pepperl+Fuchs Comtrol's Industrial Switches

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

Multiple vulnerabilities (CVE-2020-12500, CVE-2020-12501, CVE-2020-12502, CVE-2020-12503 and CVE-2020-12504) have been discovered in Pepperl+Fuchs Comtrol's RocketLinx industrial switches which may be exploited to gain access, execute commands, and obtain information. Among these vulnerabilities three of them are critical and two have been rated with high severity. One of the critical flaws allows an unauthenticated attacker to make changes to the device's configuration, upload firmware, bootloader files, and configuration files and modify network settings. Other critical vulnerability is related to the existence of multiple backdoor accounts. Another critical issue is related to the TFTP service which can be abused to read all files from the system as the daemon runs as root which results in a password hash exposure via the file /etc/passwd. OEM has released patches and workarounds to mitigate these flaws.

OEM has released patches and workarounds to mitigate these flaws.

Bad Neighbor Vulnerability in Windows TCP/IP Stack

Source: https://www.mcafee.com/

Remote code execution vulnerability occurs when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement (RA) packets. The vulnerability has been dubbed as "Bad Neighbor" because it is located within an ICMPv6 Neighbor Discovery "Protocol", using the RA type. Successful exploitation may result in an immediate BSOD (Blue Screen of Death). The effects of an exploit that would grant remote code execution would be widespread and highly impactful, as this type of bug can be made wormable. Users of Windows 10 machines are most affected. The vulnerability can be detected with a simple heuristic that parses all incoming ICMPv6 traffic, looking for packets with an ICMPv6 Type field of 134 – indicating RA – and an ICMPv6 Option field of 25 – indicating Recursive DNS Server (RDNSS). If this RDNSS option also has a length field value that is even, the heuristic would drop or flag the associated packet, as it is likely part of a "Bad Neighbor" exploit attempt. OEM has released patches for the affected products; the other workaround is to disable IPv6, either on the NIC or at the perimeter of the network by dropping ICMPv6 traffic.

The vulnerability can be detected with a simple heuristic that parses all incoming ICMPv6 traffic, looking for packets with an ICMPv6 Type field of 134 – indicating RA – and an ICMPv6 Option field of 25 – indicating Recursive DNS Server (RDNSS).

Critical Vulnerability in OpenStack Blazar Dashboard

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-26943

A user allowed to access the Blazar dashboard in Horizon may trigger code execution on the Horizon host as the user Horizon service runs under. This may lead to unauthorised access of Horizon host and further compromise of the Horizon service. It has a CVSSv3 Score of 9.9. Versions before 1.3.1, 2.0.0, and 3.0.0 are affected.

Critical Vulnerability in Juniper Networks Junos OS

Source: https://nvd.nist.gov/, https://kb.juniper.net/

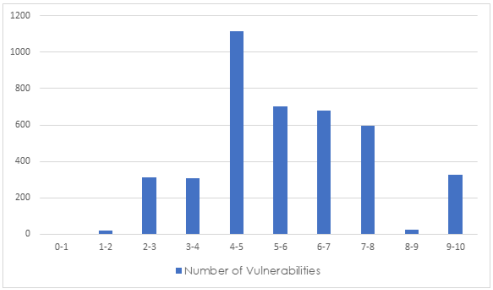
When DNS filtering is enabled on Juniper Networks Junos MX Series, receipt of specific packets processed by the Multiservices PIC Management Daemon (mspmand) process may crash (CVE-2020-1660), causing the Services PIC to reboot. While the Services PIC is rebooting, all PIC services including DNS filtering service (DNS sink holing) will be bypassed until the Services PIC boots completely. Successful exploitation may allow an attacker to cause an extended Denial of Service (DoS) attack against the device and cause clients to be vulnerable to DNS based attacks by malicious DNS servers when they send DNS requests through the device. It has a CVSSv3 Score of 9.9. Affected products are Juniper Networks Junos OS: 17.3, 18.3, 18.4, 19.1, 19.2, and 19.3.

SolarWinds SUNBURST Backdoor compromises Several Machines

Source: https://www.secpod.com/blog/, https://www.solarwinds.com/

SolarWinds software for businesses helps manage networks, systems, and information technology infrastructure. The company produces network and applications monitoring platform called Orion. This application is the recent victim of highly sophisticated supply chain attack that inserted SUNBURST malware within Orion Platform. SolarWinds.Orion.Core.BusinessLayer.dll is the digitally-signed library file known compromised, and it contains backdoor that communicates to third party servers via HTTP. Once the malware is deployed on victim's machine, after some inactive period, it retrieves and executes commands which can profile the system, transfer files, execute files, disable system services, and reboot the machine. The malware makes network traffic look like the Orion Improvement Program (OIP) protocol and stores the initially examined results within trusted plugin configuration files allowing it to blend in with legitimate SolarWinds activity. Affected versions are 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1. The OEM has removed the software builds known to be affected by SUNBURST from their download sites. It is recommended to upgrade to the latest version and to change credentials on all devices being managed by the affected SolarWinds platform.

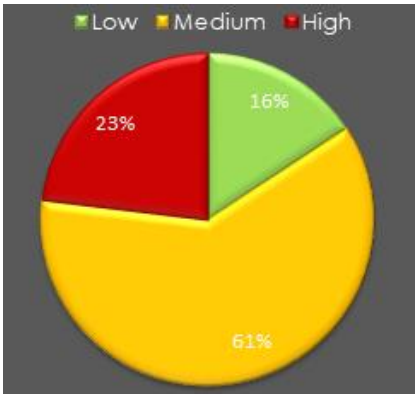
The malware makes network traffic look like the Orion Improvement Program (OIP) protocol and stores the initially examined results within trusted plugin configuration files allowing it to blend in with legitimate SolarWinds activity.



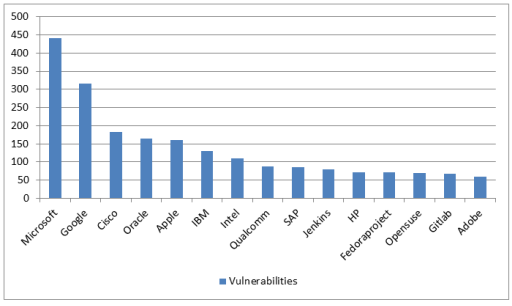
Quarterly Vulnerability Analysis Report

KMS Team, NCIIPC

A total of 4080 vulnerabilities have been observed in the month of Sep - Nov 2020. Most of the vulnerabilities had a score ranging from 4-7. 61 percent of total vulnerabilities reported were of medium severity. Microsoft, Google, Cisco, Oracle and Apple were the top five vendors.



Severity	CVSS Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Sep	Oct	Nov		
Low	0-1	0	0	0	0	
	1-2	8	9	4	21	642
	2-3	126	85	102	313	
	3-4	122	102	84	308	
Medium	4-5	441	339	333	1113	
	5-6	229	259	213	701	2495
	6-7	252	240	189	681	
High	7-8	220	189	185	594	
	8-9	3	15	6	24	943
	9-10	81	151	93	325	
Total		1482	1389	1209		4080



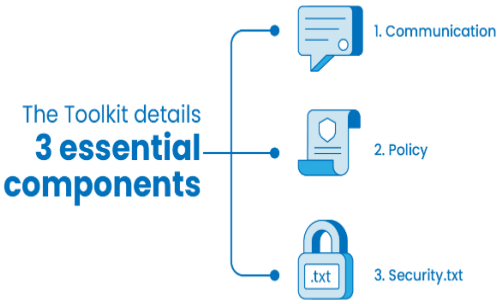
S. No.	Vendor	No. of Vulnerabilities			Total
		Sep	Oct	Nov	
(i)	Microsoft	163	125	152	440
(ii)	Google	207	37	72	316
(iii)	Cisco	76	56	50	182
(iv)	Oracle	2	160	2	164
(v)	Apple	16	126	19	161
(vi)	IBM	46	45	40	131
(vii)	Intel	2	12	95	109
(viii)	Qualcomm	37	2	48	87
(ix)	SAP	48	20	18	86
(x)	Jenkins	48	11	21	80
(xi)	HP	2	67	3	72
(xii)	Fedoraproject	25	10	36	71
(xiii)	Opensuse	40	12	17	69
(xiv)	Gitlab	39	15	13	67
(xv)	Adobe	21	21	17	59

Security App

The "Vulnerability Disclosure Toolkit"

Source: https://www.ncsc.gov.uk/; https://www.bleepingcomputer.com/

The "Vulnerability Disclosure Toolkit" is a guideline released by U.K. National Cyber Security Centre (NCSC). This document underlines the necessity for organisations of all sizes to pave the road for an open posture toward responsible bug reporting and encourage it. The guidelines are organised in three main sections that describes what can be done to direct external vulnerability information to the right person and the report follows a standard agreed framework for closing it. The components of toolkit are:



- Security.txt: this text file is hosted in the "/.well-known" directory of the domain root so that someone can easily find all the necessary information required to report a vulnerability.
- Policy: by providing a clear policy, it is defined what to be expected from someone reporting a vulnerability (as well as what you will do in response).
- Communication: having a dedicated email address or contact web form ensures that the vulnerability information gets to the right person who can help fix the issue.

This document underlines the necessity for organizations of all sizes to pave the road for an open posture toward responsible bug reporting and encourage it.

GitHub Tool Spots Security Vulnerabilities in Code

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

GitHub has developed a code-scanner that is now available for organisations using the platform as part of their software development process. The code-scanner is based on CodeQL, a code analysis technology that GitHub acquired from Semmle. The scanner helps developers to identify security vulnerabilities during development and to address the flaws before the code gets into production. After the beta release of the integrated code scanner more than 6,000 user accounts, belonging to both organisations and individuals, have enabled code scanning on their GitHub repositories. The scanner has helped discover more than 20,000 security flaws in code stored on GitHub, including remote execution flaws, SQL injection errors, and cross-site scripting flaws.

The scanner has helped discover more than 20,000 security flaws in code stored on GitHub, including remote execution flaws, SQL injection errors, and cross-site scripting flaws.

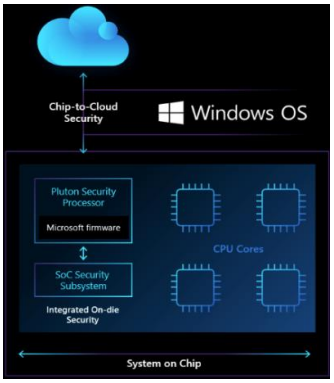
Farsight Labs Launched as Security Collaboration Platform

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

Farsight Security Inc. introduced Farsight Labs, a new collaboration platform for IT defense teams. Expander is Farsight

Expander helps digital defenders by automating the generation of regular expressions either through a web interface, or online API, or command line.

Labs first free community tool which provides a powerful method to generate patterns to discover similar domain names widely used in cyberattacks. Expander helps digital defenders by automating the generation of regular expressions either through a web interface, or online API, or command line. Expander is capable of transforming literal brand names, keywords, and search terms into regular expressions, precise patterns designed to match a search term's appearance or meaning. Defenders can use these machine-generated patterns to identify malicious activities that rely on confusing similarities. Incident responders, threat hunters, brand protection and many other digital forensics and investigation disciplines can use these regular expressions to detect and trace internet abuse, and other valuable insights for their investigations and analysis.



The technology that powers Pluton has already been used in Xbox and the Azure Sphere IoT security solution, and Microsoft now wants to implement it to Windows PCs.

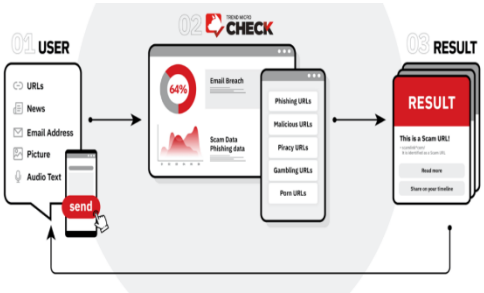
Pluton: Security Processor for PCs

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

Microsoft in partnerships with Intel, AMD and Qualcomm to release Pluton, a new security chip for Windows PCs. The technology that powers Pluton has already been used in Xbox and the Azure Sphere IoT security solution. PCs currently use the Trusted Platform Module (TPM) to store encryption keys and data required to secure the integrity of the system, but while passing through the communication channel between the TPM and the CPU the data is exposed to attacks specifically if the attacker has physical access to the targeted system. The aim of Pluton is to eliminate this threat by storing encryption keys and other sensitive data within the processor, thereby eliminating the exposure of the communication channel and providing protection against unsafe execution and other types of attacks. The integrated design of Pluton provides enhanced protection against attackers attempting to hide malicious code in the system or trying to steal encryption keys or credentials using sophisticated physical attacks.

Trend Micro Check: Tool to Tackle Misinformation

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



Trend Micro has released a free tool designed to help users secure their online privacy and fight misinformation. The tool is called Trend Micro Check; it keeps the users secure from false claims, privacy violations, and disinformation. The tool includes a Security Check that leverages threat intelligence to verify whether a website or URL is fraudulent or infected. It also implements a Privacy Check that makes use of Trend Micro's ID Security service to verify whether the email address of a user has been put up on the dark web for sale. Other features of the tool include Fact Check, which make use of the Google Fact Check API to access information from third-party fact-checking sites and verify the legitimacy of content, and News Reputation Check, which delivers

information on whether news and information websites should be trusted, based on nine basic, apolitical criteria. Trend Micro Check is capable of performing complete detection in real-time, helping users act quickly based on the results. Since its initial release this tool has been used 1.35 billion times to fight misinformation and fraud.

Trend Micro Check is capable of performing complete detection in real-time, helping users act quickly based on the results.

Mobile Security

Android/Spy23.A Malware Targeting Middle East

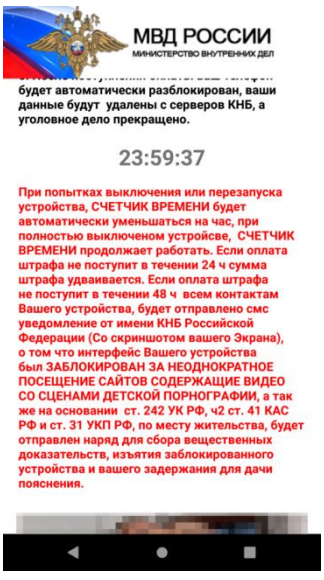
Source: https://www.welivesecurity.com

ESET researchers have discovered a new variant of Android/Spy23.A malware targeting Middle East countries. It is believed that APT-C-23 group, also known as Two-tailed Scorpion is behind this. The malware is being spread by a fake Android app store named 'DigitalApps' which contains both malicious and non-malicious apps. Three infected apps namely 'AndroidUpdate', 'Threema' and 'Telegram' are being distributed by this app store. A six-digit coupon is required to download these apps. The malware poses as popular messenger apps to lure its victims. After installation, it requests for additional permissions through sophisticated social-engineering techniques. It asks for permissions which can read users' notifications, turn off Play Protect, record user's screen under the guise of 'Message Encryption', 'Private Messages' and 'Private Video Chat' respectively. Recording audio & screen, stealing call logs & SMS messages, downloading & deleting files and uninstalling apps are some of its features. The C&C is also hidden and attacker can remotely change it. Users are advised to download genuine app from official Google Play Store only.

The malware poses as popular messenger apps to lure its victims. After installation, it requests for additional permissions through sophisticated social-engineering techniques.

AndroidOS/MalLocker.B Ransomware Detected

Source: https://www.microsoft.com/security/blog



Microsoft has detected a highly sophisticated mobile ransomware named AndroidOS/MalLocker.B which is being spread via various websites and circulated on online forums. Unlike other ransomwares, it doesn't encrypt files and block access to them. It displays a threat note as an overlay screen which blocks access to the device. Previously, ransomwares abused "SYSTEM_ALERT_WINDOW" permission to display their ransom note but later Google elevated the permission level to avoid misuse. This ransomware takes advantage of "call" notification and overrides "onUserLeaveHint()" callback method of the Android Activity to do its job. The ransomware's code also includes unused code of frozen TinyML model which gives a hint that it may try to make use of its library to produce distortion free images to make ransom notes more believable. This advanced ransomware also doesn't

include the class of obfuscated malware code in manifest file of the app. It is stored at Assets folder as a form of encrypted binary code. The decryption produces junk codes which may throw an analyst off track.


Prezado Cliente

Detectamos em nossos registros até presente data que encontra-se em aberto a fatura abaixo. Solicitamos vossa especial atenção em verificar por qual motivo este título ainda nao foi pago, antes das instruções automáticas de PROTESTO e SERASA do título.
Se já tenha sido pago, pedimos tambem nos comunicar.

FATURA: CWB-100991.5
EMISSÃO: 10/09/2020
VENCTO: 20/09/2020
VALOR: 227,32

Para sua conferencia e pagamento, segue abaixo os links para baixa-la.
Para faturas com mais de um CT-e, os arquivos XMLs e DACTEs estarão compactados em formato .ZIP

Para download da fatura em PDF, acesse neste link

Para download do XML dos CT-e 's, acesse neste link

Para download do DACTE em PDF, acesse neste link

Caso necessite dirimir dúvidas, favor entrar em contato conosco o mais breve possivel.
Estamos a sua disposição para ajudar.

It acts as a spy on one's pocket and an attacker have remote access to the victim's device to make fraudulent transactions.

Ghimob Banking Trojan

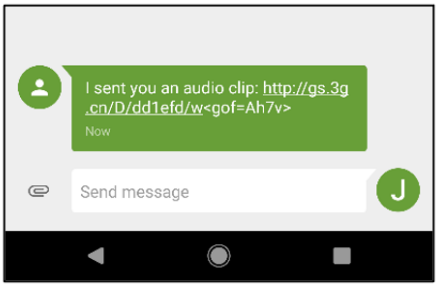
Source: https://securelist.com

Ghimob banking Trojan by Guildma threat actor is targeting 153 financial apps mainly in Brazil, Paraguay, Peru, Germany, Angola and Mozambique. It acts as a spy on one's pocket and an attacker have remote access to the victim's device to make fraudulent transactions. It even records screen lock pattern so that it can unlock the device without user's intervention. It engages the user by providing black overlays or open websites in full-windowed mode and performs banking transactions in the background. It spreads via malicious links in emails where it poses to be Google Defender app, Google Docs app, WhatsApp Updater app etc. and once opened in an Android-based browser, it downloads Ghimob apk installer. After installation, it asks for accessibility permission and once granted it disables manual uninstallation and provides remote access to the attacker. It also detects presence of emulator and debuggable flag and terminates itself. It prevents manual uninstallation, reboot and shutting down of the device by its user. The hardcoded C2s provided in the configuration file also uses 'fallback channels' technique where each hardcoded C2 is contacted to retrieve the real C2 addresses.

21 Hidden Adware in Google Play Store

Source: https://blog.avast.com

Avast has recently uncovered 21 malicious apps of over eight million downloads in Google Play Store. They pose as gaming apps which have hidden adware in them. Users are being targeted by promotion advertisements of the games in YouTube. Disguised as useful apps, this HiddenAds malware family shows intrusive ads to users outside the app. They even hide their icon to avoid detection and deletion. Before downloading any app from Google Play Store, users are advised to read reviews, pricing and permissions of the app to check whether it is a genuine app or not.



Vulnerability in GO SMS Pro

Source: https://www.trustwave.com

Popular messenger app GO SMS Pro v7.91 with more than 100 million downloads is affected by media theft vulnerability. Private voice & video messages and photos are shared in this platform. If the recipient does not have the app installed, a SMS containing a link to the media file is sent to him/ her. The content of the link can easily be viewed in a browser without any authentication or

authorisation. One can simply fuzz that link as it is sequential and predictable in nature and the contents of link can be viewed without any authorisation.

NCIIPC Initiatives

19th Meeting of Electronics and Information Technology Division Council (LITDC)

Bureau of Indian Standards (BIS) organised a webinar for Nineteenth meeting of Electronics and Information Technology Division Council (LITDC). The meeting was attended by Sh. Abhijeet Raj Shrivastava, Director NCIIPC. The brief agenda of meeting was as following:

- Scope and composition of LITDC & its panel.
- Reconstitution of sectional committees under LITD.
- Proposal for reorganisation of work of sectional committee.
- LITDC strategic road map.
- Review of activities.
- Important standards developed/under development by LITD.
- International activities.
- Product certification.
- Quality control orders.
- Information on e-sale of standards by BIS.

Webinar on Cyber Security in CII by NCIIPC and THDC

A Webinar was organised by Tehri Hydro Development Corporation (THDC) on 29 Oct 20 at 1500 hrs and lecture was delivered by NCIIPC on "Cyber Security in Critical Information Infrastructure." The Webinar was attended by more than 35 participants from THDC. Further Ms. Seema Mittal, Director (P&E) delivered lecture on "Cyber Security in Critical Information Infrastructure" and covered the following topics:

- Critical Information Infrastructure (CII)
- Threats to CII - Impact of an attack in IT & OT infrastructure and steps to be taken to reduce such attacks
- Cyber Security in CII:
  - Prevent Malware in delivery
  - Limit the extent of Cyber Security Incidents
  - Detect Incidents and Respond
  - Recover Data and System Availability
  - Preventing Malicious Insiders
  - Ransomware Prevention Strategy
  - Cyber Security Deception

Dr. Ajeet Bajpai, DG NCIIPC addressing SecCon APJC 2020

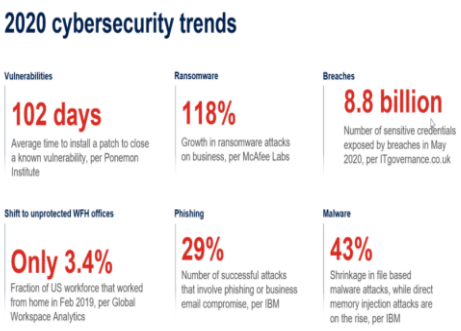
NCIIPC's participation in SecCon APJC 2020

Dr. Ajeet Bajpai, DG NCIIPC spoke on "Securing Indian Cyberspace - Trends, Threats and Challenges" at SecCon APJC 2020 organised by Cisco. The event was held on 16th October, 2020. SecCon APJC 2020 global program was designed to integrate security awareness, security experts, and networking opportunities to create powerful lasting connections and advancements helping Cisco maintain their position as a security leader. Ms. Rama Vedashree, CEO of Data Security Council of India, spoke on "Cybersecurity as a Strategic Pillar for a Growing Digital Economy"; Mr. Vanja Svajcer, Technical Leader for Cisco Talos, spoke on "Cisco Talos and threats in times of COVID-19"; Mr. Al Huger, Vice President and General Manager of the Security Platform and Response unit at Cisco, spoke on "Secure X"; and Mr. John Maynard, Vice President of Global Security Sales Cisco, spoke on "Decoding Zero trust in a Pandemic Environment". The SecCon APJC 2020 provided attendees with training and cutting-edge information to build upon their existing security skills.

DSCI-ZNet Virtual Panel Discussion on 'Five Vectors of Holistic Cyber Protection Strategy'

The Data Security Council of India (DSCI), in association with ZNet Technologies, organised an exclusive live virtual panel discussion on theme 'Five Vectors of Holistic Cyber Protection Strategy' on November 12, 2020, and same was attended by Ms. Poornima Malagimani, Coordinator South, NCIIPC. The webinar focused on adopting a holistic approach to fight cybercrimes as a topmost priority for businesses. The session focused on the holistic approach encompassing the five vectors - SAPAS (Safety, Accessibility, Privacy, Authenticity, and Security). The session covered the following aspects:

- Deep-dive into SAPAS.
- Case of LockerGoga ransomware – a multi-stage attack or "living off the land" (LoTL) tactic that allow hackers to hide their attacks as legitimate processes.
- Today's threat landscape from cybersecurity experts.
- Ways cybercriminals and ransomware get into your system. Know about phishing, DDoS, XSS, SQL injection, malware, spyware, MITM, and more from experts.
- Relate whether having just a backup or anti-virus can save business. Understand why traditional approaches to cyber protection are dead.
- Deliberate on why one needs to adopt a comprehensive cyber protection approach with the best cyber protection solutions to mitigate the risks associated with today's modern threats.



NCIIPC in Bengaluru Tech Summit 2020

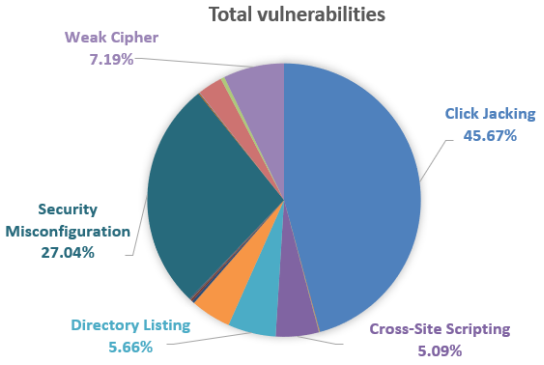
NCIIPC participated in an interesting panel discussion on the topic "Implementing Responsible Vulnerability Disclosure Program for Government Sector" during Bengaluru Tech Summit 2020 held from 19th Nov to 21st Nov 2020. Dr. Ajeet Bajpai, DG NCIIPC was one of the panel members including Ms. Katie Moussouris, Founder & CEO, Luta Security; Mr. Nandankumar Saravade, CEO, ReBIT; and Mr. Sachinraj Shetty, Head of Information Security, Ola.

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 1572 vulnerabilities reported during 11 Sep to 24 Nov 2020. Following are the top 10 vulnerabilities:

- Click Jacking
- Security Misconfiguration
- Weak Cipher
- Directory Listing
- Cross-Site Scripting
- E-mail Spoofing
- SQL Injection
- Using Components with Known Vulnerabilities
- HTML Injection
- Broken Authentication
- Insecure Direct Object Reference (IDOR)



Around 266 researchers participated in RVDP programme during 11 Sep to 24 Nov 2020. NCIIPC acknowledges following top 15 researchers for their contributions during 11 Sep to 24 Nov 2020 for protection of National Critical Information Infrastructure:

- Nikhil Kumar
- M V Vaishnav Rajeevan
- Kailas Patil
- Mitali Singh
- Yash Mahajan
- Nirjhar Banik
- Kislay Kumar
- Abhijit Nayak
- Dhiraj V Ramteke
- Srikar
- Sachin Mishra
- Divyanshu Kumar
- Raghotham Mruthike
- Aditya Sharad Bhosale
- Vaibhav Lakhani

Upcoming Events - Global

JANUARY 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

FEBRUARY 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	23	23	24	25	26	27
28						

January 2021

- FloCon 2021, Virtual — 12-15 Jan
- 13th International Conference on Global Security, Safety & Sustainability, Virtual — 14-15 Jan
- FutureCon Detroit Cyber Security Conference — 20 Jan
- International Conference on Cybersecurity and Security Systems, Paris — 25-26 Jan
- FutureCon Orange County CyberSecurity Conference, Virtual — 27 Jan
- IT-Defense 2021, Berlin — 27 Jan
- Women in Cloud Annual Summit, Redmond — 30 Jan

February 2021

- Cyber Security for Critical Assets MENA, Dubai — 1-2 Feb
- ManuSec Europe Summit, Munich — 2-3 Feb
- International Conference on Cybersecurity and Cybercrime, Bangkok — 4-5 Feb
- HackCon 2021, Oslo — 17-18 Feb
- 17th Annual SecureWorld New England Virtual Conference, Virtual — 18 Feb
- Third Party & Supply Chain Cyber Security Summit 2021, Madrid — 18-19 Feb
- 2nd International Artificial Intelligence and Blockchain Conference (AIBC), Macau — 24-26 Feb
- International Conference on Cyber Resilience and Information Security, Buenos Aires — 25-26 Feb

March 2021

- Techno Security & Digital Forensics Conference Colorado 2021, Denver — 9 Mar
- Cybercon London 2021, London — 9 Mar
- FutureCon Minneapolis CyberSecurity Conference, Minneapolis, and Virtual — 10 Mar
- International Conference on Advances in Internet of Things Technologies, Miami — 11-12 Mar
- Passive and Active Network Measurement 2021, Cottbus — 28 Mar
- Virtual Cybersecurity Summit: Connected Devices Security — 30-31 Mar
- FutureCon Boston CyberSecurity Conference, Boston and Virtual — 31 Mar

April 2021

- International Conference on Organisational Cybersecurity and Cyberresilience, Cancun — 5-6 Apr
- Cybertech Global UAE 2021, Dubai — 5-7 Apr
- SecureWorld Mid-Atlantic Virtual Conference — 8 Apr
- Rethink! IT Security D/A/CH, Berlin — 19-20 Apr
- CyberTech Tel Aviv 2021, Tel Aviv — 20-22 Apr
- FutureCon Omaha CyberSecurity Conference, 2021Omaha, and Virtual — 21 Apr
- OffZone 2021, Moscow — 22-23 Apr
- FutureCon San Antonio CyberSecurity Conference, San Antonio and Virtual — 29 Apr

Upcoming Events - India

- 13th International Conference on Communication Systems & Networks, Bengaluru — 5-9 Jan
- 4th International Conference on Recent Advancements in Engineering & Technology, New Delhi — 29-30 Jan
- International Conference on Cybersecurity of Smart Grids 2021, Mumbai — 8-9 Feb
- NULLCON 2021, Goa — 10 Mar
- Virtual Cybersecurity Summit: India & SAARC — 23-24 Mar
- FinTech India Expo 2021, New Delhi — 24-26 Mar
- Convergence India 2021, New Delhi — 24-26 Mar
- 2nd International Conference on Technological Innovations in Engineering & Management, Visakhapatnam — 30-31 Mar
- 2nd International Conference on Future Communication & Computing Technology 2021, Mumbai — 29-30 Apr

MARCH 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	23	23	24	25	26	27
28	29	30	31			

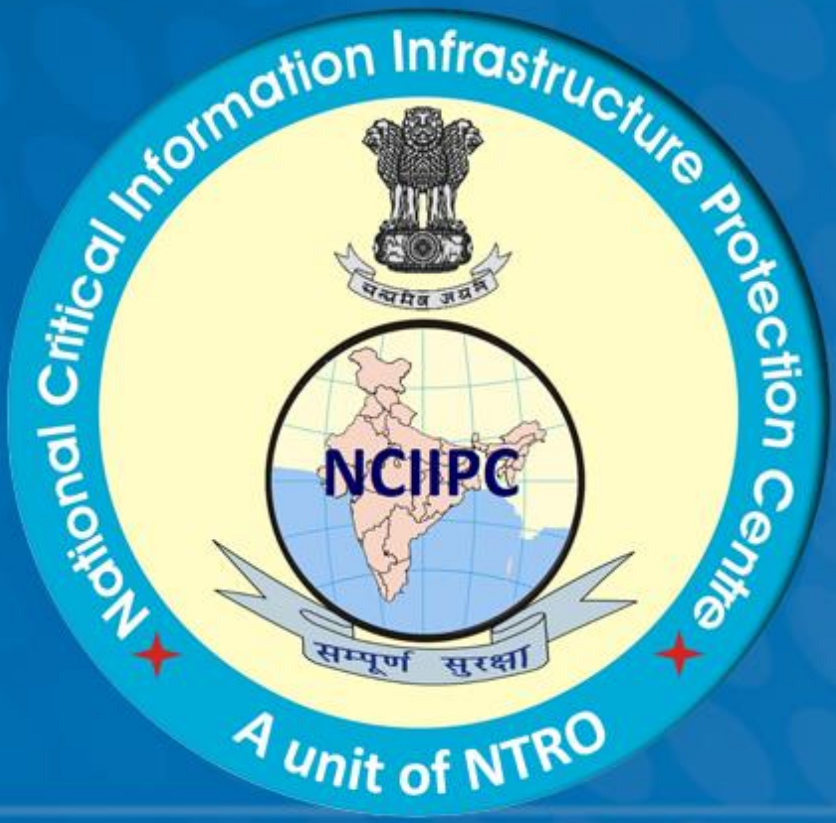
APRIL 2021

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	

NULLCON

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

Notes



Feedback/Contribution

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

Disclaimer

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