NEWSLETTER

October 2020

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

Ministry of Housing and Urban Affairs
Government of India

> "The dream of Swachhata cannot be achieved even if 100 Mahatma Gandhis or 1000Narendra Modis come together, but if 125 crore Indians come together that dream can easily be fulfilled."
>
> Narendra Modi, Prime Minister

On the day of Swachh Bharat Mission let's also pledge for Swachh Cyber Bharat to create a Safe, Strong and Resilient Cyber Space for Indian Citizens to prosper.

BEST CYBER HYGIENE PRACTICES

1 USE ANTIVIRUS SOFTWARE

2 UPDATE SOFTWARES REGULARLY

3 SECURE YOUR NETWORK

4 BACKUP YOUR DATA FREQUENTLY

5 USE MULTI-FACTOR AUTHENTICATION

6 BEWARE OF PHISHING SCAMS

7 CONTROL APP PERMISSIONS

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

VOLUME 4 ISSUE 4

@NCIIPC

NCIIPC Newsletter

October 2020

Inside This Issue

Message from the NCIIPC Desk

Hon'ble Prime Minister of India, Sh. Narendra Modi, during his Independence Day address to the nation, announced that India would soon have new Cyber Security Strategy. There is also a growing concern around the globe regarding Supply Chain contamination of cyber security products manufactured in certain geographical regions. India has immense potential to serve as a trusted supply chain partner. The PM exhorted the Indian industry to raise the bar from 'Make in India' to 'Make for the World'.

National Security Advisor, Sh. Ajit Doval, addressing an international virtual conference, in his Keynote Address, reiterated the resolve to secure the cyber space for social and economic wellbeing.

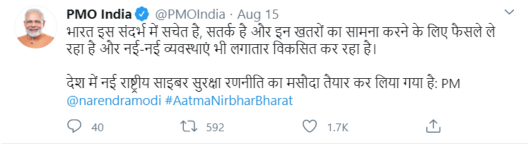
The Overseas Key Information Database (OKIDB) leaked by Christopher Balding has been in the news lately. OKIDB has been developed by Shenzhen Zhenhua Data Information Technology. The firm is reported to be mining information not only on important personalities across the globe but also information pertaining to near real-time movement of warships, satellite tracking, troop movements and similar activities. While the implications are still being analysed, it would be reasonable to assume that in future, Big Data Surveillance Systems will play a significant role in global geo-politics.

COVID-19 pandemic continues unabated. Likewise, threat actors continue to propagate targeted email phishing, vishing and other attacks related to COVID-19 theme targeted towards India's critical sector organizations.

In this issue, we bring in guest article on 'Risk Assessment at Enterprise Level'. Researchers around the globe are putting their best efforts to come up with innovative ideas to identify and mitigate enterprise cyber security risks.

Comments, suggestions and feedback are solicited from the readers. Selected letters shall also be published. You may write to us at newsletter@nciipc.gov.in

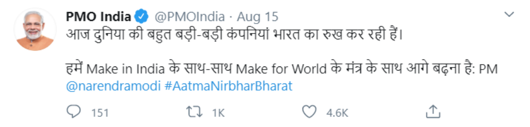
We wish our readers a healthy and safe festive season ahead.



PMO India @PMOIndia · Aug 15
भारत इस संदर्भ में सचेत है, सतर्क है और इन खतरों का सामना करने के लिए फैसले ले रहा है और नई-नई व्यवस्थाएं भी लगातार विकसित कर रहा है।

देश में नई राष्ट्रीय साइबर सुरक्षा रणनीति का मसौदा तैयार कर लिया गया है: PM @narendramodi #AatmaNirbharBharat

40 592 1.7K



PMO India @PMOIndia · Aug 15
आज दुनिया की बहुत बड़ी-बड़ी कंपनियां भारत का रुख कर रही हैं।

हमें Make in India के साथ-साथ Make for World के मंत्र के साथ आगे बढ़ना है: PM @narendramodi #AatmaNirbharBharat

151 1K 4.6K

News Snippets - National

India and Israel Sign Agreement to Deal with Cyber Threats

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

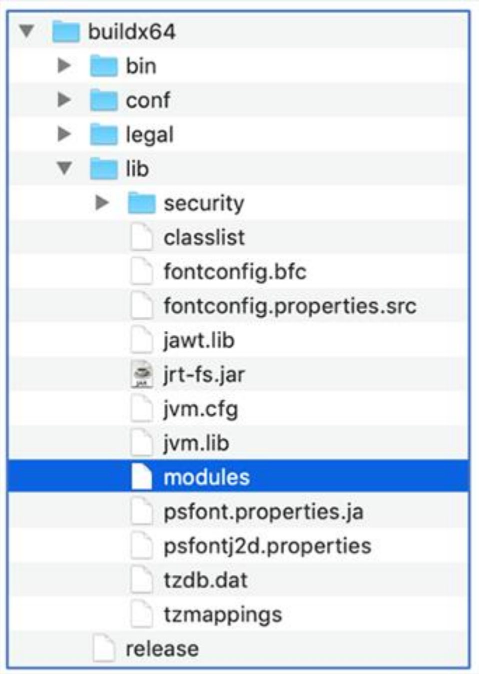
India's Ambassador to Israel, Sanjeev Singla and Director-General of Israel's National Cyber Directorate (INCD), Yigal Unna signed an agreement to further expand collaboration in dealing with cyber threats amid rapid digitisation due to the coronavirus pandemic that exposed the vulnerabilities of the virtual world. The MoU signed between the Indian Computer Emergency Response Team (CERT-In) and INCD deepens the operational cooperation between the two sides and will expand the scope of information exchange on cyber threats in order to raise the levels of protection in the field. Director-General of INCD states "Israel can contribute from its experience and can benefit from the vast experience gained in India in dealing with cyber-attacks".

> *"Israel can contribute from its experience and can benefit from the vast experience gained in India in dealing with cyber-attacks"*

CERT-In Warned About New Tycoon Virus Targeting PC's

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

The Indian Computer Emergency Response Team (CERT-In) released a public alert about new ransomware called "Tycoon" that is targeting Windows and Linux systems. This ransomware found by BlackBerry Threat Intelligence and UK Cyber Response Services is said to be a multi-platform Java-based malware that can be used to encrypt both Windows and Linux devices. The initial stage of the attack involves the attackers connecting to the systems using an RDP server on the network. Tycoon ransomware comes in the form of a ZIP archive containing a Trojanized Java Runtime Environment (JRE) build. The malware is compiled into a Java image file (JIMAGE) located at lib\modules within the build directory. After encrypting important files and data of businesses, the attackers claim for ransom in Bitcoins. CERT-In is advising users to disable their RDP if not in use. "If required, it should be placed behind the firewall and users are to bind with proper policies while using the RDP.



```
▼ buildx64
    ▶ bin
    ▶ conf
    ▶ legal
    ▼ lib
        ▶ security
          classlist
          fontconfig.bfc
          fontconfig.properties.src
          jawt.lib
          jrt-fs.jar
          jvm.cfg
          jvm.lib
          modules
          psfont.properties.ja
          psfontj2d.properties
          tzdb.dat
          tzmappings
      release
```

Contents of zip file (Source: blogs.blackberry.com)

Hackers Attack J&K Power Department Data Center

Source: https://news.abplive.com/

The data centre of Jammu and Kashmir Power department was rendered in-operational due to a cyber-attack. The website of the department, http://billsahuliyat.jkpdd.net/ and its Android app both were affected. According to Neel Kamal Singh, Executive Engineer, IT wing of Power Department, through a particular kind of cyber-attack, named 'Ransomware', all the official files and data were encrypted. To prevent accessing further uncompromised data and servers of the department, all the network data lines were closed. Four servers were compromised, which department was unable to access, as attackers retained the key with them.

Four servers were compromised, which department was unable to access, as attackers retained the key with them.

Cyber Attack on NHAI Email Server, No Data Loss

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

A cyber-attack took place on National Highways Authority of India (NHAI) email server, but the prompt action resulted in no data loss. As a precaution, the Authority shut down the server. NHAI Chief General Manager, Akhilesh Srivastava, told "A ransom ware attack on NHAI email server took place. The attack was foiled by the security system and email servers were shut down from safety point of view. No data loss took place. NHAI data and other systems remained unaffected from this attack,".

Chinese Eyeing Information on India's Defence and Research

Source: https://zeenews.india.com/

The Chinese Army's secret unit '61398' which is known for cyber espionage, engaged in gathering information like cyber, space and geolocation intelligence around the world for a long time has intensified its activities eyeing information related to India's defence and research, the security agencies sounded an alert. Icebug, Hidden Lynx (a professional advanced persistent threat using the program) and APT-12 have been used for attacking government and industrial organization by Chinese hackers. Many cases had been reported in the last few months in which Chinese hackers associated with the PLA attempted to gather sensitive information of the country through cyber espionage.

Icebug, Hidden Lynx (a professional advanced persistent threat using the program) and APT-12 have been used for attacking

News Snippets - International

FBI Warns of NetWalker Ransomware Targeting Businesses

Source: https://www.waterisac.org/, https://www.securityweek.com/

The Federal Bureau of Investigation (FBI) agency of United States received notifications of Netwalker ransomware attacks on government organizations, education entities, private companies, and health agencies. Cyber actors using Netwalker have taken advantage of the COVID-19 pandemic to compromise an increasing number of unsuspecting victims. Netwalker encrypts all connected Windows-based devices and data, rendering critical files, databases, and applications inaccessible to users. When executed, Netwalker deploys an embedded configuration that includes a ransom note, ransom note file names, and various configuration options. Netwalker spread through a Visual Basic script attached to COVID19 phishing e-mails that executed the payload once opened. Netwalker is using Pulse Secure VPN (CVE-2019-11510) and Telerik UI (CVE-2019-18935) vulnerabilities. Once an actor infiltrated a network with Netwalker, a combination of malicious programs may be executed to harvest administrator credentials, steal valuable data, and encrypt user files. In order to encrypt the user files on a victim network, the actors typically launch a malicious PowerShell script embedded with the Netwalker ransomware executable.

Netwalker have taken advantage of the COVID-19 pandemic to compromise an increasing number of unsuspecting victims

Israel Foiled Cyber Attack on Its Defence Firms

Source: https://threatpost.com/

The Israeli defence ministry told that it had foiled an attempted cyber-attack by a foreign group targeting the country's defence manufacturers. It said the attempt was made by "an international cyber group called 'Lazarus,' an organisation that is backed by a foreign country."

Ministry of Defense

Australia Launches New Cybersecurity Strategy

Source: https://hstoday.us/

The Australian Cyber Security Strategy 2020 will invest $1.67 billion over 10 years to achieve the government's vision of creating a more secure online world for Australians, their businesses and the essential services upon which they all depend. While the new strategy is an Australian government initiative, the government recognizes the essential role of state, territory, local governments, businesses, academia, international partners and the broader community in strengthening Australia's cyber security. Every part of government, business and the community have a role to play in implementing the Cyber Security Strategy 2020.

Australian Government

AUSTRALIA'S CYBER SECURITY STRATEGY 2020

Targeted BEC Attacks Steal Business Data in Six Countries

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

A targeted business email compromise (BEC) orchestrated by the Russian-speaking RedCurl group has successfully stolen information in 14 successful attacks on a variety of businesses – mostly construction companies, financial and consulting firms, retailers, insurance businesses, law firms and travel in six countries. The attackers nicked employee profiles, client information and construction plans. RedCurl attempts to remain on a victim's network as long as possible, usually for 2-6 months, said Rustam

RedCurl attempts to remain on a victim's network as long as possible, usually for 2-6 months.

Mirkasymov, a threat intelligence expert at Group-IB, which released a report on the campaign.

US Warns of North Korean Hackers Targeting Banks Worldwide

BeagleBoyz have been using malicious remote access tools as part of ongoing attacks to steal millions from international banks

Source: https://www.bleepingcomputer.com

North Korean hackers tracked as BeagleBoyz have been using malicious remote access tools as part of ongoing attacks to steal millions from international banks according to a joint advisory issued by several US Government agencies. The joint release says that North Korea's BeagleBoyz hacking group has once again started robbing banks through remote Internet access since February 2020.

New Zealand Stock Exchange Targeted by DDoS Attacks

New Zealand's stock market was interrupted by an apparent overseas cyber-attack for two days.

Source: https://www.theguardian.com/

New Zealand's stock market was interrupted by an apparent overseas cyber-attack for two days. The Wellington-based NZX exchange went offline and although some connectivity was restored for investors, some trading was halted. The NZX said it had experienced "network connectivity issues" and that the NZX main board, NZX debt market and Fonterra shareholders market were placed on halt.

Trends

Honeywell Sees Rise in USB-Borne Malware

These Snippets of malware can launch DoS attacks, which cause the operations management networks to lose sight and harm or interrupt key properties

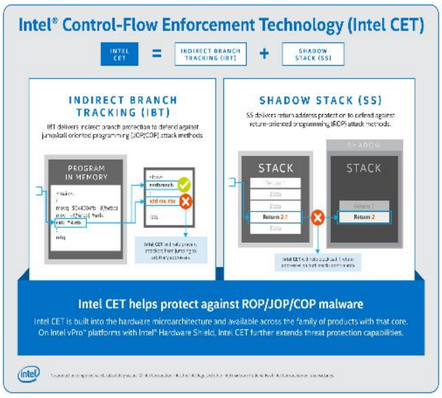
Source: https://www.securityweek.com/

Honeywell industrial cybersecurity issued its 2020 USB threat report which was predicated on data collected over a period of twelve months by the company's Secure Media Exchange, USB security platform from different industrial sites across 60 countries in America, Europe and Asia. The percentage of malware found on USB drives that was especially designed to target industrial systems dropped from 14% to 11% compared to 2018 report. If ransomware is considered, the 11% becomes 28% that has targeted Operational Technology (OT) systems. These Snippets of malware can launch DoS attacks, which cause the operation management networks to lose sight and harm or interrupt key properties. An analysis of the data showed that there is an increase in the percentage of viruses, trojans, rootkits and worms and a drop in potentially unwanted applications, non-targeted bots, adware, spyware and hacking instruments. Now a days the strategy for an attacker is to gain a foothold via USB in industrial environments.

New Security Tech in Intel CPUs Protects Systems Against Malware

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

Intel recently revealed a new security technology for its processors that will help protecting systems against attack methods commonly used by malware. The new Control Flow Enforcement Technology (CET) that is forged into the hardware micro-architecture, will initially be available in Tiger Lake mobile processors, but Intel plans on including it in both desktop and server platforms in the future. The new Control Flow Enforcement Technology has two main components: indirect branch tracking (IBT) and Shadow Stack (SS). The IBT provides protection against Jump-Oriented Programming (JOP) and Call Oriented Programming (COP) attacks and SS provides return address protection against Return-Oriented Programming (ROP) attacks. Malware often recons on control-flow hijacking to reach its goals and many pieces of software are affected by memory safety issues that leads to these types of attacks. Intel has been working with Microsoft to create better protections provided by CET through a feature called Hardware-enforced Stack Protection against these types of attacks.


Intel® Control-Flow Enforcement Technology (Intel CET)
INTEL CET = INDIRECT BRANCH TRACKING (IBT) + SHADOW STACK (SS)
INDIRECT BRANCH TRACKING (IBT)
IBT delivers indirect branch protection to defend against jump/call oriented programming (JOP/COP) attack methods.
PROGRAM IN MEMORY
endbranch
SHADOW STACK (SS)
SS delivers return address protection to defend against return-oriented programming (ROP) attack methods.
STACK
Return 2.1
SHADOW STACK
Return 2
Intel CET helps protect against ROP/JOP/COP malware
Intel CET is built into the hardware microarchitecture and available across the family of products with that core. On Intel vPro® platforms with Intel® Hardware Shield, Intel CET further extends threat protection capabilities.

The new Control Flow Enforcement Technology (CET) for Intel processors will help protecting systems against attack methods commonly used by malware.

US Unveils Blueprint for 'Virtually Unhackable' Internet

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

A report has been unveiled by Department of Energy (DOE) officials that pushes out a blueprint strategy for the development of a national quantum internet, using laws of quantum mechanics to send information more securely than on existing networks. The agency has been collaborating with universities and industry researchers on the engineering for the initiative with the aim of creating a prototype within a decade. Recently Scientists from DOE and the University of Chicago built a 83 kilometer "quantum loop" in the Chicago suburbs, establishing one of the longest land-based quantum networks in the nation. The objective is to establish a more secure network based on quantum "entanglement," or the transmission of sub-atomic particles. Scientists from DOE plan to use the trait of quantum transmissions in which it is exceedingly difficult to eavesdrop on as information passes between locations to make virtually unhackable networks.

U.S. DEPARTMENT OF ENERGY
LAUNCH TO THE FUTURE
QUANTUM INTERNET
Fermilab
THE UNIVERSITY OF CHICAGO
Argonne NATIONAL LABORATORY

A blueprint strategy for the development of a national quantum internet, using laws of quantum mechanics to send information more securely than on existing networks.

A Billion User Hours Lost in European Union (EU) Telecom

Telecom Sector, NCIIPC

The national telecom security authorities in Europe reported 153 major telecom security incidents in the year 2019. The reported incidents had a whole impact of almost 1 billion user hours lost. Incident report is important to understand various cyber security functions and controls and helps to develop the correct security measures.

- System failures dominate in terms of impact. This category is almost half (48%) of the user hours lost. However, the frequency and overall impact of system failures are trending down significantly over the past 4 years. More than a quarter, 26% of total incidents reported due to human errors as root cause. The same has increased by 50% compared to the previous year.
- 32% of the incidents are due to third-party failure. This implies that these incidents originated at third parties, typically utility companies, contractors, suppliers, etc. This number is tripled compared to 2018.
- Looking inside the category of system failures, hardware failures are very significant. Almost quarters of incidents (23%) were reported due to hardware failures and have very high on user hours, amounting 38%.
- Power cuts and failures are still very critical and it is either primary or the secondary cause over one fifth of the major incidents.

Incident report is important to understand various cyber security functions and controls and helps to develop the correct security measures.

References:

[1] https://www.enisa.europa.eu/news/enisa-news/annual-report-on-telecom-security-incidents-in-2019

[2] https://cip-association.org/a-billion-user-hours-lost-in-eu-telecoms-due-to-security-incidents-in-2019/

Critical Information Infrastructure in Indian Health Sector

Sector Coordinator, NCIIPC

Health Information Technology (HIT) is application of information processing involving computer hardware and software dealing with storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making. India is one of the leading countries in the fields of medicine research & development, bioinformatics software development, automation of various bio-instrumentation methods, medical records aggregation, and database management for various Government health programs. In accordance with National Health Policy which recognizes the integral role of technology in healthcare, Government of India has taken multiple initiatives to improve healthcare access and encourage robust healthcare industry. The policy advocates extensive deployment of digital tools for improving efficiency and outcome of healthcare system. It aims at an integrated health information system which serves all stake-holders and improves efficiency, transparency, and citizen experience. However, such widespread use of Information Technology also brings in risks that are related to Information Security.

The policy advocates extensive deployment of digital tools for improving efficiency and outcome of healthcare system. It aims at an integrated health information system which serves all stake-holders and improves efficiency, transparency, and citizen experience.

There are four major areas to focus on from the perspective of securing critical health information technology in India:

- Government Systems and Records: This impact decision making through various policies, strategies, budget allocations, investments and also in the management of national health infrastructure.
- Networks and Equipment used in research: May result in loss or theft of valuable intellectual property.
- Automation in Manufacturing: May result in serious quality deficit issues.
- Health Information Records: May result in improper treatments, incorrect diagnosis as well as loss of privacy.

In addition, compromise to any such system, may lead to loss of trust in the system, resulting in reputation loss leading to various indirect consequences like trade, international investments, interruption in sharing/supply of resources from other countries.

The National Health Policy 2017 requires a Health Technology Assessment to ensure that technology choice is participatory and is guided by considerations of scientific evidence, safety, consideration on cost effectiveness and social values. This framework needs to include the identification of critical business and industrial processes and their underlying critical information infrastructure (CII), which has to be done by the respective stakeholders in the Health sector. It is important that organisations in this critical sector adopt the best practices of Information Security to protect their critical processes and the underlying information infrastructure, which may already be existing or in the process of getting established.

Identification of risks to the critical business and industrial processes and analysis of the impact of large-scale cyber-attacks on their underlying CII will enable necessary prioritization and informed decision making.

A few key aspects that stakeholders should consider are:

- Risk and Impact Analysis: Identification of risks to the critical business and industrial processes and analysis of the impact of LARGE-SCALE CYBER-ATTACKS on their underlying CII will enable necessary prioritization and informed decision making.
- Policies and Systems: These include the design and implementation of Information Security best practices through policies and systems such as Information Security Management Systems (ISMS), Business Continuity and Cyber Crisis Management, IT and OT Asset Management, systems and network architecture resilience and so on.
- People and Processes: A large number of breaches into the information architecture occur due to ignorance or malicious

intent of people, as well as through gaps in processes.

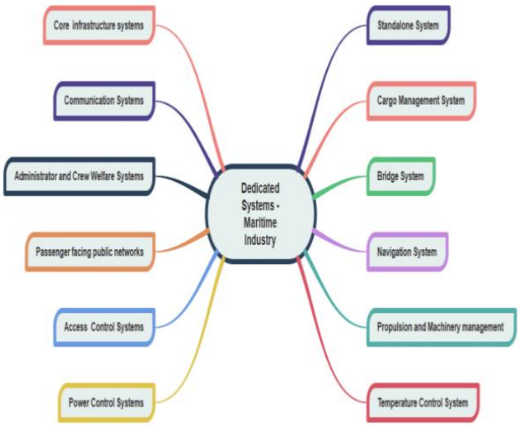
- Technology and Security Services: Organisations should leverage the core technologies that are available for securing their information infrastructures, using their internal resources as well as specialized services from information security service providers.

A large number of breaches into the information architecture occur due to ignorance or malicious intent of people, as well as through gaps in processes.

Cyber Security Challenges in Maritime Operational Technologies

Transport Sector, NCIIPC

The maritime industry, which includes shipping companies, cargo carriers, and cruise lines is undergoing a digital transformation in their operations. The systems used in the shipping Industry increasingly depend upon collaboration of IT and OT on board the ships as well as their connection to the Internet. This opens a larger attack surface to the maritime OT systems, which include:


Dedicated Systems - Maritime Industry
Core infrastructure systems
Communication Systems
Administrator and Crew Welfare Systems
Passenger facing public networks
Access Control Systems
Power Control Systems
Standalone System
Cargo Management System
Bridge System
Navigation System
Propulsion and Machinery management
Temperature Control System

- Vessel Integrated Navigation System (VINS)
- Global Positioning System (GPS)
- Satellite Communications
- Automatic Identification System (AIS)
- Radar systems and Electronic charts

Recently Observed Tactics, Techniques, and Procedures on OT:

- Spear phishing to get initial access to the organization's information technology network before entering to the Operational Technology network.
- Deployment of commodity ransomware to encrypt data in IT and OT networks.
- Connecting to Internet Accessible Programmable Logic Controllers which requires no authentication for initial access.
- Use of Commonly Used Ports and Standard Application Layer Protocols, to communicate with controllers and download control logic.
- Utilizing vendor engineering software and Program Downloads.
- Modifying Control Logic and Parameters on PLCs.

Examples of cyber threats that affect the maritime industry include SATCOM hacking and Navigational System Spoofing. Satellite communications systems are prone to frequent cyber-attacks. Maritime Navigational Systems receive data via radio frequency transmission at sea. Attackers can manipulate or distort signals to send a vessel off course without detection of changes, potentially causing a collision or allowing hackers to hijack the vessel's GPS. While dealing such type of cyber threats, it is important to consider the uniqueness of OT systems, as these assets control the physical world. Cyber Security challenges in Maritime OT are as follows:

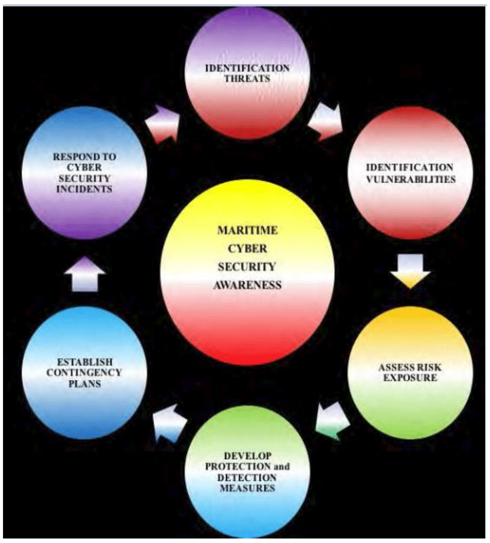
- OT systems are responsible for real-time performance, and response to any incident is critical to time to ensure the high reliability of the systems.

- Access to OT systems should be strictly controlled without interrupting the required human-machine interaction.
- Safety of these systems is of greatest importance, and fault tolerance is essential. Even the minute downtime may not be acceptable.
- OT systems present extended diversity with unshared protocols and operating systems, often without embedded security capabilities.
- They have long lifecycles, and any updates or patches to these systems must be carefully designed and implemented to avoid impacting reliability and availability.
- The OT systems are designed to support the required operational process and may not have memory and computing resources to support the addition of security capabilities.

> *Maintaining effective Cybersecurity is not just an IT issue but is rather a fundamental operational assertive in the 21st century maritime environment.*

Impacts:

- A cyber-attack that manipulate chart data held in Electronic Navigational Charting Systems (e.g. ECDIS) or misdirects GPS signals can cripple vessels and also effect the safety of onboard personnel, ships, and cargo.
- Loss or manipulation of external sensor data that is critical to the operation of a ship.
- Effecting Loss of Availability on the OT network.
- Resulting in Loss of Productivity and Revenue.
- Adversary Manipulation of Control and destruction of physical processes.


IDENTIFICATION THREATS
IDENTIFICATION VULNERABILITIES
ASSESS RISK EXPOSURE
DEVELOP PROTECTION and DETECTION MEASURES
ESTABLISH CONTINGENCY PLANS
RESPOND TO CYBER SECURITY INCIDENTS
MARITIME CYBER SECURITY AWARENESS

Recommendations:

- Have a Resilience Plan for OT
- Harden Your Network
- Implement an Accurate "As-operated" OT Network Map Immediately
- Understand and Estimate Cyber-risk on "As-operated" OT Assets
- Design and Implement a Continuous and Vigilant System Monitoring Program

References:

[1] https://fortressinfosec.com/building-a-sustainable-maritime-ot-cyber-security-program/

[2] httpss://fairplay.ihs.com/safety-regulation

[3] https://www.tripwire.com/state-of-security

[4] https://www.fireeye.com/blog/threat-research/2020/03/monitoring-ics-cyber-operation-tools-and-software-exploit-modules.html

[5] https://media.defense.gov

[2] https://www.securitymagazine.com/articles/93187-how-to-prioritize-security-and-avoid-the-top-10-iot-stress-factors??v=preview

[3] https://www.arcweb.com/market-studies/internet-things-railwa

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

RDAT Backdoor Used by OilRig group as Steganography Technique

Threat Assessment Group, NCIIPC

OilRig is an Iranian threat group which primarily targets variety of industries including financial, government, energy, chemical, and telecommunications largely focusing operations in Middle East region. Attacker behind this group mainly relies on social engineering to exploit rather than software vulnerabilities; however, the group has used recently patched vulnerabilities in the delivery phase of their attacks on occasion. The steganography technique of RDAT tool is used for employing novel email-based Command and Control (C2) channel in order to hide commands and data within bitmap images attached to emails while exfiltrating data. Recently, research reports have revealed that the Greenbug group having similar feature of OilRig involved in targeting telecommunications organisations in Southeast Asia specifically using downloaders, custom Bitvise, Mimikatz tools, and a custom backdoor RDAT. Previously, it was seen that RDAT tool was first uploaded to the TwoFace webshell and further with active development, RDAT resulted in multiple variations of the tool that rely on both HTTP and DNS tunnelling for C2 communications. The ability to use Exchange Web Services (EWS) to send and receive emails for C2 communications has been added recently by developer of RDAT. It becomes much more difficult to detect and allow for higher chances of defence evasion due to combination of using emails with steganographic images to carry the data across the C2 can result in this activity being.

The ability to use Exchange Web Services (EWS) to send and receive emails for C2 communications has been added recently by developer of RDAT.

References:

[1] https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/

[2] https://threatpost.com/oilrig-apt-unique-backdoor/157646/

[3] https://attack.mitre.org/groups/G0049/

Malware Bytes

PROMETHIUM Extends Global Reach with StrongPity3 APT

Source: https://threatpost.com/

APT group known as StrongPity is spreading again with its watering-hole campaign, mainly targeting Kurdish victims in Turkey and Syria. This group (a.k.a Promethium) offers trozanised version of various file recovery application, remote-connection applications, security software such as 7-zip, WinRAR archiver, TeamViewer etc. through a series of misleading website. Victim of this campaign is selected by pre-defined IP list, hiding inside malicious installer's configuration file. Malware once installed over victim machine has file-searching mechanism searching through drives, looking for files with specific extension. Further, all these searched files are placed in a temporary .ZIP archive and divided into hidden .SFT encrypted files, sent to the C2 server. The group uses a multi-tiered C2 infrastructure, first layer is a Pool of IPs for connecting with the malware. These IP are proxies to other machine uses PHP curl bindings to forward the request to next server. They use HTTPS protocol for communication with TCP port 1402. The first layer IP forward data to second layer IP addresses, with multiple first-layer IPs pointing to them. As, an additional layer actor use secureconnect.me and torguardvpnaccess.com for connecting the server.

Malware once installed over victim machine has file-searching mechanism searching through drives, looking for files with specific extension.

Chinese Malware 'Golang' Targeting Windows & Linux Machines

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

Golang, a new variant of cryptominer is aimed at mining Monero, an open-source cryptocurrency. The spotted IP addresses linked with this malware are related to China, targeting both Windows and Linux machine. This malware spreads by scanning the internet for vulnerable machines. Instead of targeting end-users, Golang focuses on attacking web application framework, application servers, and services such as Redis and MSSQL. Once the malware infects the machine, it downloads the file, based on the platform it is attacking. For windows machine, a backdoor is also added by malware. The 'Go' programming language also referred as GoLang is well-known in the hacker community, since it is not commonly tracked by antivirus software. It targets vulnerable servers which is the top threat vector that cybercriminals look to exploit. To protect from such malware, organisations need a web application firewall with proper configuration, as well as monitoring the end points for suspicious activity and CPU usage.

Instead of targeting end-users, Golang focuses on attacking web application framework, application servers, and services such as Redis and MSSQL.

Alien Malware Can Steal Passwords From 226 Apps

Source: https://www.techradar.com/

ThreatFabric researchers have discovered a new malware named Alien that has ability to steal passwords from 226 apps. It is based on source code of gang malware also named as Cerberus. It can be purchased as a Malware-as-a-Service on hacker forums on dark web. The Alien malware has capability to overlay attacks, control and steal SMS messages and harvest the contact list. This malware can use its keylogger for any use and therefore is able to broaden its attack scope further than its target list. It has ability to install, remove and start applications on an infected device. It also captures the notifications on infected device and offers RAT feature. Alien malware can also be used to show fake login pages for 226 Android apps which allows it to steal banking credentials easily from infected devices. Alien malware is distributed using a variety of methods including fake apps, phishing sites, and SMS.

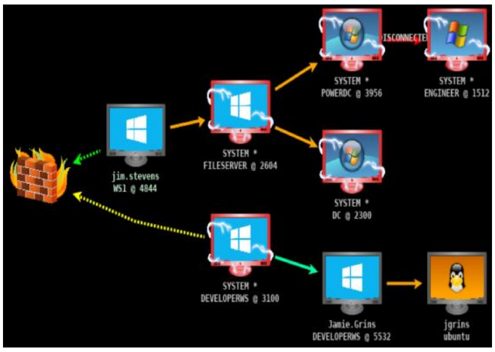
Image source: https://www.threatfabric.com/

This malware can use its keylogger for any use and therefore is able to broaden its attack scope further than its target list.

India and Hong Kong Targeted with New Variant of Malware

Source: https://blog.malwarebytes.com/

A Chinese state-sponsored hacking group targeted India and Hong Kong with a unique phishing attack. The archive file with an embedded document pretends to be from Government of India. The file uses a new variant of Cobalt Strike to drop a malicious template. The downloaded template uses the dynamic data exchange (DDE) protocol to execute malicious commands, which are encoded within the document's content. Threat actors used certutil to download a com scriptlet from its server and used Squiblydoo technique to execute downloaded scriptlet via regsvr32.exe on the victim's machine. Scriptlet uses VB macro and calls Excel to execute it. It uses reflective DLL injection method to embed payload into rundl32.exe. Further, the threat actor changed the template and dropped loader called as MgBot. This MgBot executes and injects its final payload through the use of Application Management service on Windows. To make analysis harder, the malware includes several anti-analysis and anti-virtualization techniques. It avoids running in a known virtualized environment. Researchers have found several malicious android applications that are part of toolset used by this APT group.



To make analysis harder, malware includes several anti-analysis and anti-virtualization. It avoids running in a known virtualized environment.

GoldenSpy Campaign Tries to Erase Evidence of Malware

Source: https://www.scmagazine.com/

Trustwave SpiderLabs discovered a new malware family, known as GoldenSpy. This malware is found embedded in tax payment software that Chinese bank requires corporations to install to conduct their business operation. During investigation it was found that tax payment software installed a hidden backdoor on the system that enabled a remote adversary to execute Windows commands or to upload and execute any binary. GoldenSpy installs two identical versions of itself, both as autostart services. The tax software uninstall feature will not uninstall GoldenSpy. It leaves GoldenSpy running as backdoor. It does not contact tax software's network infrastructure directly, rather it reaches through another domain. It randomizes beacon time to avoid network security technologies to identify beaconing malware. It runs with system level privileges, making it highly dangerous and capable of executing any software on the system.

Lazarus Hackers Deploy Ransomware, Steal Data

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

North Korea based hacking group known as Lazarus is active with its new malware framework known as MATA, targeting corporate entities of various countries. MATA is a modular framework with several components including a loader and multiple plugins. It can be used to infect Windows, Linux and macOS systems. During attack MATA load plugins into the infected system's memory running commands, manipulating files and processes, injecting DLLs, creating HTTP proxies and tunnels on windows devices. After fully deployment of malware it tries to find database with sensitive customer or business information. It runs database queries to collect and exfiltrate customer lists. It has been found that MATA is linked with Manuscrypt trojan due to similar configuration data such as randomly generated session ID, date-based version information, a sleep interval and multiple C2s and C2 server addresses.

After fully deployment of malware it tries to find database with sensitive customer or business information.

CISA, DOD, FBI Exposed New Chinese Malware Named Taidoor

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

Taidoor, a malware family associated with Chinese state-sponsored hackers targets private entities. Taidoor, also known as Taurus RAT, has 32-and 64-bit system versions installed on victim's systems as a service Dynamic Link Library (DLL). This DLL contain two other files, first file is a loader which is started as a service. Loader, further decrypts the second file and executes it in memory, which is main Remote Access Trojan (RAT). It allows hackers to access infected systems and exfiltrate data or deploy other malware. It normally deployed together with proxy servers to hide the true point of origin of the malware's

It normally deployed together with proxy servers to hide the true point of origin of the malware's operator.

operator. To strengthen the security posture of an organization, the administrator should configure firewall to deny unsolicited connection requests and maintain appropriate access control lists.

IcedID Trojan Rebooted with New Evasive Tactics

BFSI Sector, NCIIPC

A novel banking trojan named as IcedID has been causing havoc among financial institutions across the US, UK and Canada, including banks, mobile services providers and e-commerce sites. IcedID has some resemblance with other banking trojans such as Zeus, Gozi, and DRIDEX with common features such as the use of web injection and redirection techniques. The delivery method of this malware is via botnet infrastructure of EMOTET. During the COVID-19 pandemic this banking Trojan was spotted with a new functionality to help it avoid detection and standard security protection. In a recent phishing attack campaign documents were trojanized by the widely used banking trojan IcedID. Attackers sent phishing emails to potential victims, allegedly from the accounting department. The emails incorporated an invoice with a password-protected ZIP file attached. This password protection allows the file to escape from anti-malware solutions. The campaign also included a curious behavior wherein it rotated the file name used for the attachment inside the ZIP file, which seems to be an "useless" attempt to escape security protections. Once users opened the attachment, a three-stage attack was launched to unleash the Trojan:

The delivery method of this malware is via botnet infrastructure of EMOTET.

- The expanded ZIP files have a document with macro that executes after opening the document. Once macros are enabled, a script downloads the Dynamic Link Libraries (DLL) and saves it as a PDF.
- This DLL downloads the succeeding stage of the attack from the loadhnichar[.]co as a PNG file and decrypts it.
- Stage three ultimately downloads the IcedID main module as a PNG file, spawns a msiexec.exe process and injects the IcedID main module into it

How to avoid installation of Malware:

- Carefully analyse each attachment received in mail. If the mail received is from stranger or sender seems to be suspicious then do not open attachments.
- Update your operating system, browsers, and plugins.
- Install Antivirus and enable auto update.

References:

[1] https://threatpost.com/icedid-trojan-rebooted-evasive-tactics/158425/

[2] https://www.trendmicro.com/vinfo/pl/security/news/cybercrim
and-digital-threats/icedid-banking-trojan-targets-us-financial-institutions

[3] https://blog.malwarebytes.com/101/2016/08/10-easy-ways-to-prevent-malware-infection/

How Dharma Ransomware-as-a-Service (RaaS) Model Works

BFSI Sector, NCIIPC

Small businesses organizations are facing a number of Ransomware threats because the programs needed to launch such attacks become more widespread. The group named Dharma and their affiliates are focusing on getting smaller ransom payments from victim organizations. All ransomware attacks spotted by hackers now a days are taking advantage of vulnerabilities in Remote Desktop Protocol (RDP) which is used by system administrators and employees to connect to corporate networks remotely.

Majority of Dharma attacks can be controlled by ensuring RDP servers are patched and secured behind a VPN with multifactor authentication (MFA).

Menu of Variants: Dharma features a large menu of variants and a criminal ecosystem for the RaaS offering. Cybercriminals are performing the targeted attacks, with the help of standard toolkits. With the COVID-19 pandemic forcing most organisations to start remote working, there is a sharp increase in brute-force and other attacks, that look to exploit unpatched RDP connections to get access into corporate networks. These Ransomware operators don't allow affiliates to possess full control over the decryption keys. Victims contact the attackers with the help of a tool that is used to extract information about the files that were encrypted into a document. The encrypted document then pasted into email and is sent back to the affiliates who submit that data through a portal to the RaaS to obtain the actual keys. Once their payment has been received, a typical ransomware affiliate will get access to a toolkit having the malware and instructions for performing the tasks. When the remote connection is created, the tools that are residing in directory on the threat actor's computer, is mapped to the target network as an accessible network drive. The directory contains variety of customized hacking tools and freeware versions of a variety of legitimate system utilities together with the Ransomware executable files.

Recommendation: Majority of Dharma attacks can be controlled by ensuring RDP servers are patched and secured behind a VPN with multifactor authentication.

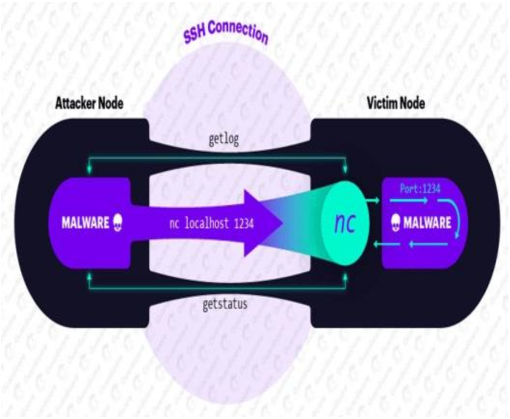
References:

[1] https://www.techradar.com/in/news/dharma-ransomware-as-service-poses-major-threat-to-smbs

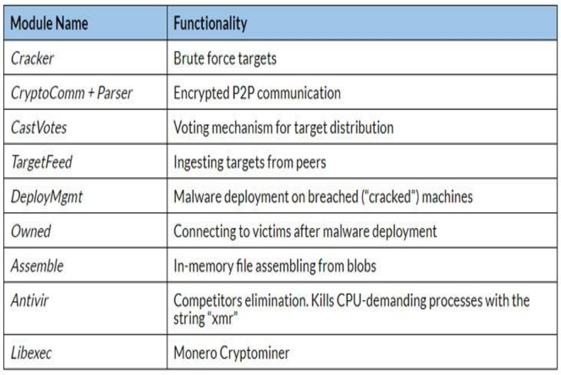
[2] https://www.bankinfosecurity.com/how-dharma-ransomware-as-a-service-model-works-a-14826

P2P Botnet Malware

Power and Energy Sector, NCIIPC



P2P Botnet Malware is capable of brute-force attacks to break into SSH servers and spread to tens of millions of IP addresses belonging to Critical Infrastructures entities. P2P Botnet malware can establish backdoor connection on victim machines which grants regular access for the attackers. After identifying target machines, the P2P Botnet malware can perform various tasks including brute-force attack, infecting the machine with malicious payloads upon a successful breach, and adding the victim to the P2P network. These botnets have centralized command-and-control infrastructure. With its decentralized infrastructure, it distributes control among all its nodes on the network. Every node is capable to target the systems and also to communicate with each other (including update), on encrypted channel. P2P Botnet Malware is very robust and can run any executable file or script on attacking machines.



Module Name	Functionality
Cracker	Brute force targets
CryptoComm + Parser	Encrypted P2P communication
CastVotes	Voting mechanism for target distribution
TargetFeed	Ingesting targets from peers
DeployMgmt	Malware deployment on breached ("cracked") machines
Owned	Connecting to victims after malware deployment
Assemble	In-memory file assembling from blobs
Antivir	Competitors elimination. Kills CPU-demanding processes with the string "xmr"
Libexec	Monero Cryptominer

Module Names and its Functionalities of P2P Botnets

Challenges: There are various challenge in P2P botnet malware as below:

- In the P2P botnet malware, there is always constant flow monitoring at a node, which results in a major computational challenge.
- Specifying the network profile of P2P bots is nontrivial as different botnets exhibit different semantics and protocols
- Differentiating between the behavior of a normal node and a P2P bot is a complex problem.

Recommendations: Due to P2P Botnet malware's distributed nature (commands can be sent to and from any node in the network), tracking of P2P botnet's operators is a complicated task. These are the recommendations for getting over these type of botnet malwares.

- Choosing strong passwords

- Using safer public key authentication
- Use of Captcha
- Password policy may be limited to minimum number of login attempts.
- Changing the SSH port or completely disabling SSH access if the service is not in use.

References:

[1] https://www.guardicore.com/2020/08/fritzfrog-p2p-botnet-infects-ssh-servers/

[2] https://www.bankinfosecurity.com/how-dharma-ransomware-as-a-service-model-works-a-14826

[3] https://www.zdnet.com/article/new-fritzfrog-p2p-botnet-has-breached-at-least-500-enterprise-government-servers/

[4] https://www.zdnet.com/article/new-fritzfrog-p2p-botnet-has-breached-at-least-500-enterprise-government-servers/

KONNI Malware

Transport Sector, NCIIPC

KONNI is a Remote Access Trojan (RAT) used by malicious cyber actors to steal files, gaining control keystrokes, take screenshots, and execute arbitrary code on infected systems. The KONNI malware family is potentially linked to APT37, a North-Korean cyber espionage group it often delivered via phishing emails as a Microsoft Word document with a malicious Visual Basic Application (VBA) macro code.

Impact: Attackers may try to gain unauthorized access to steal files, capture keystrokes, take screenshots and arbitrary code execution on victim's system.

Execution flow: KONNI is usually delivered through spear-phishing campaigns, which are highly targeted and private as compared to traditional phishing attacks. The targeted nature of the attack makes it difficult to detect the attack, even by the most tech savvy users. The malicious code can change the font colour from light grey to black (to fool the user to enable content), to ascertain if the Windows OS is a 32-bit or 64-bit version, and construct and execute instructions to download additional files. Once the VBA macro builds the instructions, it uses CertUtil, the certified database tool to download remote files from a given Uniform Resource Locator (URL). It also uses a built-in function to decipher base64-encoded files. Finally, the attacker removes the document from the temp directory and executes the .BAT file.

> *KONNI is usually delivered through spear-phishing campaigns, which are highly targeted and private as compared to traditional phishing attacks.*

KONNI is additionally ready to collect the IP address and usernames, delete files, create shortcuts to masquerade as legitimate files, and gather architecture data, connected drives, hostname, and computer name from the victim's machine. The malware has been observed using the File Transfer Protocol to exfiltrate reconnaissance data from the victim's system. A hacker also can use a RAT to take control of a home network and make a botnet. Basically, a botnet allows a hacker to use the PC resources for illegal tasks, like as DDoS attacks.

Hackers are leveraging a phishing campaign to deploy KONNI Malware, a Remote Access Trojan (RAT) to steal data, capture keystrokes, take screenshots and launch cyber-attacks.

How to Prevent:

- Keep antivirus software and operating system patches up to date
- Deactivate file and printer sharing services. If these services are required then use strong passwords or Active Directory authentication.
- Limit end-user permissions and prevent users from installing and running unwanted software applications
- Develop and implement a password policy
- Leverage firewalls
- Track users' web browsing habits
- Disable unnecessary services on workstations and servers.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the Internet prior to execution.
- Maintain situational awareness of the latest threats and implement appropriate access control lists.

References:

[1] https://us-cert.cisa.gov/ncas/alerts/aa20-227a

[2] https://malpedia.caad.fkie.fraunhofer.de/detail/win.konni

[3] https://www.msspalert.com/cybersecurity-breaches-and-attacks/malware/dhs-konni-malware-warning/

[4] https://medium.com/d-hunter/a-look-into-konni-2019-campaign-b45a0f321e9b

[5] https://healthitsecurity.com/news/dhs-cisa-alerts-to-phishing-campaign-to-deploy-konni-rat-malware

BLINDINGCAN Malware

Transport Sector, NCIIPC

BLINDINGCAN is a remote access Trojan (RAT) also called as DRATzarus deployed by North Korea's wicked Lazarus and APT38 Group targeting US and foreign businesses that are operating actively in the military defence and aerospace sectors. This malware gains access to the victim's system, perform reconnaissance, and then gathers intelligence of surrounding key military and energy technologies.

Infection Process: The hackers impersonate recruiters from big corporations and lure employees into an interviewing process and ask them to open (malicious) Office or PDF documents through Phishing emails. The emails contain malicious attachments that deploy the Trojan on the victim's machine when the victim opens the files. It contains macros that attempt to connecting external domains to download Trojan and install it. Sometimes phishing emails contains DLL files. These DLL files attempt to install another DLL file that unpack and run the BLINDINGCAN Trojan. Once hackers gain access to the victim's system, they perform reconnaissance to gather intelligence of military, aerospace and energy technologies. This BLINDINGCAN Malware has the capability to gather the following information:

BLINDINGCAN Malware can gain unauthorized access to victim's systems to perform reconnaissance of Defence and Aerospace sectors.

- Retrieve information about all installed disks, including the disk type and the amount of free space on the disk
- Get Operating System (OS) version information
- Get Processor information
- Get system name
- Get local IP address information
- Get the victim's Media Access Control (MAC) address.
- Create, start, and terminate a new process and its primary thread
- Search, read, write, move, and execute files
- Get and modify file or directory timestamps
- Change the current directory for a process or file
- Delete malware and artifacts associated with the malware from the infected system

How to Prevent:

- Keep up-to-date antivirus signatures and engines.
- Ensure operating system patches are up-to-date.
- Disable all the file and printer sharing services.
- Use robust passwords or Active Directory authentication.
- Stop users from installing and operating undesired software applications.
- Execute regular password changes.
- Scan properly before opening e-mail attachments, even if the attachment is required, and the sender appears to be a known person.
- Allow a personal firewall on company workstations, configured to deny undesirable connection requests.
- Disable unnecessary services on agency workstations and servers.

Practice caution while using removable media. Examine all software that are downloaded from Internet prior to administering it.

- Browse for and eliminate suspicious e-mail attachments.
- Check the users’ web browsing habits; restrict access to sites with unsuitable content.
- Practice caution while using removable media.
- Examine all software that are downloaded from Internet prior to administering it.
- Manage situational perception of the latest threats and perform appropriate Access Control Lists (ACLs).

References:

[1] https://www.zdnet.com/article/cisa-warns-of-blindingcan-a-new-strain-of-north-korean-malware/

[2] https://cybersecuritynews.com/u-s-gov-exposed-north-korean
remote-access-trojan/

[3] https://www.izoologic.com/2020/09/02/defense-on-north-korean-blindingcan-malware/

[4] https://www.infosecurity-magazine.com/news/us-reveals-north
korean/

[5] https://www.bleepingcomputer.com/news/security/us-govt-exposes-new-north-korean-blindingcan-backdoor-malware/

[6] https://cyware.com/news/north-korean-hackers-using-blindingcan-malware-strain-dhs-sounds-alert-83986e9d

[7] https://www.computing.co.uk/news/4019206/north-korean-blindingcan-malware

Transparent Tribe Targets Government and Military Using USB

Threat Assessment Group, NCIIPC

Transparent Tribe is a Pakistan based cyber espionage APT group that tries to collect intelligence from the Indian government and military employing a new tool to infect USB devices and unfold to different systems. It is predicted in recent analysis that APT has shifted its focus to Afghanistan. PROJECTM and MYTHIC LEOPARD are different aliases of Transparent Tribe that is involved in large scale cyber espionage campaigns. Like different APT’s, Transparent Tribe also begin its attack via spear-phishing emails. The group uses Crimson RAT as main payload that is put in via malicious documents containing embedded macros sent with fraudulent messages. If victim clicks on malicious document and permits macros, the custom .NET Trojan is launched and performs functions like connecting to Command-and-Control(C2) server for data exfiltration, stealing files, harvest credentials stored in browsers, capturing screenshots, stealing files and compromising microphones &

webcams. Transparent Tribe also uses Python-based Trojan referred to as zippy, however new USB attack tool is of major interest. USBWorm has two vital elements, a file stealer for removable drives and a worm feature for moving to new vulnerable machines. If a USB device is connected to an infected machine, a Trojan is quietly put in on the removable drive. A duplicate of Trojan is buried within the root drive directory that are listed by the malware on the drive. The directory attribute is modified to "hidden" and a fake Windows icon is employed to lure victims. Once user try to access directories by clicking on icon a payload is executed that hides all the actual directories and replace them with copy of malware using the same directory name. Transparent Tribe is extremely focussed cyber threat group perpetually evolving its toolkit depending on the intended target to add in its arsenal.

> *USBWorm has two vital elements, a file stealer for removable drives and a worm feature for moving to new vulnerable machines. If a USB device is connected to an infected machine, a Trojan is quietly put in on the removable drive.*

Recommendation:

- Use up-to-date antivirus programs that can detect and prevent a wide range of malware, trojans, and viruses, that APT hackers can use to exploit system.
- To control malicious activity always use rules to block advanced macro activity, process creation, process injection commenced by Office applications.
- Use network firewall and Windows Defender Firewall to prevent any communication among endpoints.
- Monitor for clearing of Event Logs, particularly the safety Event log and PowerShell Operational logs.

References:

[1] https://www.zdnet.com/article/transparent-tribe-hacking-grou spreads- malware-by-infecting-usb-devices/

[2] https://www.proofpoint.com/sites/default/files/proofpoint-operation- transparent-tribe-threat-insight-en.pdf

Chinese APT Group Emissary Panda targeting Government

Threat Assessment Group, NCIIPC

Emissary Panda also known as APT-27, HIPPOTeam, TG-3390, Group-35, Bronze Union, ZipToken, TEMP.Hippo, Iron Tiger APT, BRONZE UNION, Lucky Mouse is a China-based threat actor that involves in targeting foreign embassies to collect data related to government, defence, and technology sectors. Activity of Emissary Panda has been noticed since 2010 during attack in organisations across the world including financial services firms, US defence contractors, and a national data center in Central Asia. The group aimed at new generation weapons and in surveillance activities on dissidents and other civilian groups during cyber espionage campaigns the group target their victim by leveraging both readily available tools and custom malware in their operations. In recent attack, the group has updated code in its tools in addition to tools which was available for years. Attacker behind this group uploads a variety of tools to perform various activities like dumping credentials, and locating and pivoting to additional systems on the network. Previous, Emissary Panda had used list of legitimate applications such as cURL, custom backdoors such as Hyperbro post-exploitation tools like Mimikatz and tools to scan for and exploit potential vulnerabilities in the target network.

Attacker behind this group uploads a variety of tools to perform various activities like dumping credentials, and locating and pivoting to additional systems on the network.

Recommendations:

- Filter email correspondence and scrutinize attachments for malware.
- Make regular backups of system and store the backups offline, preferably offsite so that data cannot be accessed via the network.
- Have a well-thought-out incident response and communications plan.
- Strongly consider instituting role-based access, limiting organisation-wide data access, and restricting access to sensitive data.
- Implement basic incident response and detection deployments and controls like network IDS, netflow collection, host logging, and web proxy, alongside human monitoring of detection sources.

References:

[1] https://securityaffairs.co/wordpress/86316/apt/emissary-panda middle-east-gov.html

[2] https://otx.alienvault.com/

ELDERWOOD: The Chinese APT Group

Threat Assessment Team, NCIIPC

Elderwood is a Chinese cyber espionage group that attacked Google in 2009 using Hydraq Trojan horse known as Operation Aurora and Google also confirmed that some of its intellectual property had been stolen. Interesting highlights of their approach include: the use of seemingly unlimited amount of zero-day exploitation, attacks on service providers working for the target organization. This group mainly uses spear-phishing emails and web injections in watering hole attacks (compromising certain websites likely to be visited by the target organization) for initial compromise and targets source code of the applications using reverse engineering to identify the new vulnerabilities. The targeted sectors include large numbers of

This group mainly uses spear-phishing emails and web injections in watering hole attacks for initial compromise and targets source code of the applications using reverse engineering to identify the new vulnerabilities.

Aeronautics, Defence, Education, Energy, Engineering, Financial, NGOs, Supply Chain Manufacturer, IT and Shipping. The most attacked countries are Australia, Canada, Denmark, Hong Kong, India, Switzerland, Taiwan, UK and USA. The most talked about and dangerous attack carried out by the group came in September 2017, when ELDERWOOD used CCleaner Version 5.33 to deliver malware. CCleaner is an application used for periodic maintenance of systems that include temporary file cleaning, system analysis to determine how to improve the system performance. To identify CCleaner target, they targeted download servers used by the software vendor to distribute the official software package which was linked to deliver malware to unexpected victims. For some time, the official signed version of CCleaner 5.33 distributed by Avast used to contain malware uploads mounted on top of CCleaner installer. At the time of installation of the CCleaner 5.33, a 32-bit CCleaner binary was also installed and contained a malicious payload with a Domain Generation Algorithm (DGA) as well as hardcoded Command and Control (C2) functionality. CCleaner recorded over 2 billion total downloads in November 2016 at a development pace of an extra 5 million clients for each week. Because of the potential damage that could be caused by an infected computer network or a small fraction of this size on September 13, 2017 Cisco Talos immediately informed Avast of the findings so that they could begin appropriate response activities.

To identify CCleaner target, they targeted download servers used by the software vendor to distribute the official software package which was linked to deliver malware to unexpected victims.

Prevention from watering hole and phishing attack:

- In watering hole attack, attackers create fake websites (same look and feel like original) loaded with malware. These websites trick the legitimate users into entering their names and passwords, or downloading malwares.
- This technique is mainly used for companies with high security in their email accounts and Internet access, making cybercrime very difficult.
- While these types of attacks can be performed through many types of software, the most targeted software includes Adobe Reader, Flash, and Internet Explorer. If possible, then one must remove all these software's from system.
- Use of a secure Virtual Machine for launching web browser in a virtual environment will limit access to the local system, and can stop watering hole attacks from succeeding.
- By using two-factor authentication, such as a numeric code generated by a token, makes it much harder for hackers to

In watering hole attack, attackers create fake websites (same look and feel like original) loaded with malware. These websites trick the legitimate users into entering their names and passwords, or downloading malwares.

break into your system.

- Don't open any email or attachment which seems suspicious.
- Deploy a web filter to block malicious websites.
- Always use updated applications with improve security patches.
- Use firewalls and Antivirus.

References:

[1] https://www.infopoint-security.de/medien/the-elderwood-project.pdf

[2] https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

[3] https://www.itsasap.com/2018/07/31/5-ways-defend-watering-attacks/

Researchers Exploited a Bug in Emotet to Stop its Spread

Source: https://thehackernews.com/2020/08/emotet-botnet-malware.html

Emotet an email-based banking trojan acting behind botnet-driven spam campaign and ransomware attacks has a flaw that allowed researchers to kill it and prevent it from spreading. Behaving like a Swiss Army knife it can work as a downloader, information stealer, and spambot depending on how it is deployed. Recently, it developed a new feature to identify and compromise fresh victims connected to infected device nearby wi-fi networks. It randomly chose exe or dll filename from the system32 directory to save the malware on victim system. It encrypts filename with an XOR key and save it to the window registry value. Killing mechanism developed by researchers, employed a PowerShell script that generate the registry key value for each victim and set the data for each value to null. Thus, whenever malware check the registry for filename it would end up loading an empty .exe, stopping the malware from running on the target system. Improvised version of kill-switch also called as EmoCrash was able to exploit buffer

Recently, it developed a new feature to identify and compromise fresh victims connected to infected device nearby wi-fi networks. It randomly chose exe or dll filename from the system32 directory to save the malware on victim system.

Guest Article

Quantifying Cyber Security Risk at an Enterprise Level

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

It is well known that a Risk Based approach is the most recommended practice to manage cyber security in enterprises. It involves conducting technical as well as operational (or process) Risk Assessment to arrive at a Measure of Risk (MoR). As per the prevalent and widely accepted international standards, 'Risk' is a function of Impact (adverse) of an event and likelihood of occurrence of the event. The severity of 'Impact' being determined by value of asset, the degree of threat and vulnerabilities of the system in question. Thus, the Measure of Risk (MoR) for an individual Information System (IS), is a function of four factors, namely the value of asset, threats, vulnerabilities and the likelihood of the threats exploiting the vulnerabilities; the likelihood being measured by the effectiveness of controls (or the absence of them) put in place to protect the assets.

The above guidelines, however, do not specify how and in what manner these four factors are actually combined to arrive at the risk computed for a single Information system; nor do they specify how MoR for individual information systems are combined to provide an overall Measure of Risk for an Enterprise as a whole. This article attempts to suggests a method of computing a quantity for the measure of risk for the enterprise as a whole.

Why an Enterprise level MoR is needed: An Overall, enterprise-wide 'Measure of Risk' is needed, because it allows the board or the senior management of the enterprise to adequately and appropriately allocate resources. It is also needed to see the trend over a number of years or to compare the progress made in reducing risk vis-à-vis previous years. The MoR at the enterprise level can be used to verify whether the allocated budgets and resources to implement the controls have actually resulted in effectively reducing Risk and, if so, by how much.

Measure of Risk for an individual Information System: As mentioned earlier, standards and accepted guidelines state four factors to arrive at the Measure of Risk for an individual information system, namely:

- Asset Value (AV)
- Threats (T)
- Vulnerabilities (V)
- Likelihood/Probability of Occurrence (POO)

While the factors listed above can be combined in various ways, it is suggested that for every individual Information System, the Measure of Risk be a multiplied product of these four factors, as:

MoR = AV x T x V x POO

Asset Value: Asset value can be given a quantitative value based on the 'Criticality' of the equipment being considered, as elaborated in a previous article on the subject. We had suggested that there be 5 categories based on the criticality namely 'Most Critical', 'Critical', 'High Value', 'Important' and 'Others'. These categories could be assigned a value on a scale of 5, from 5 to 1 in that order, thus giving an Asset Value of 5 to the Most Critical assets and so on.

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.

Asset	Value
Most Critical	5
Critical	4
High Value	3
Important	2
Others	1

Table: (a)

Threat	Value
High	3
Medium	2
Low	1

Table: (b)

Vulnerability	Value
High	3
Medium	2
Low	1

Table: (c)

POO	Value
Most Likely	3
Likely	2
Less Likely	1

Table: (d)

MoR (AVxTxVxPOO)	Risk Rating	Risk Score for IS
90 < MoR <= 135	HIGH	5
30 < MoR <= 6	Medium	3
6< MoR <=1	Low	1

Table: (e)

Enterprise Level MoR	Enterprise Level Risk Rating
0 <= MoR < 2	Low
2 <= MoR <=4	Medium
4< MoR <= 5	High

Table: (f)

Let M = No of systems with Risk Rating 'MEDIUM', with Risk Score 3;

Let L = No of systems with Risk Rating 'LOW', with Risk Score 1;

Enterprise Level Risk Score = [(H x 5) + (M x 3) + (Lx1)]/ N.

For example, out of 100 Information Systems, say 23 had 'HIGH' risks, 48 had 'Medium' ratings and remaining 29 had Low ratings, the enterprise level risk rating would be computed as: [(23 x 5) + (48 x 3) + (29 x 1)]/ 100 which works out to 2.8, which can be categorised as 'Medium', as per the table given in table (f).

Conclusion: Most enterprises undertake cyber security risk management activities regularly and rather well. While Measure of Risk for individual information systems are worked out well, it would go a long way to enhance the confidence of the senior management, the board and senior executives such as CISO to know the overall risk rating for the enterprise as a whole. This would enable them, to know to a greater degree of accuracy, as to where their enterprise stands with regard to cyber security, what is their risk score, how was it when compared to the past year, whether there has been an improvement and if so to confirm (or otherwise) that the security measures implemented and the budgets spent have been effective in reducing the measure of risk.

Learning

When Any.Run is fed with a malware sample, it creates a Windows virtual machine with an interactive remote desktop and the file is executed.

Malware Authors Develop New Method to Evade Analysis

Source: https://cyware.com

Any.Run is an interactive malware analysis sandbox that allows researchers to analyse any malware safely, without risking their systems. Any.Run is a dynamic malware analysis tool that provides total control over the malware activity and can affect it in a few clicks, unlike an automated malware analysis tool. When Any.Run is fed with a malware sample, it creates a Windows virtual machine with an interactive remote desktop and the file is executed. This assists the researchers to observe the behaviour executed by a malware. The behaviour of a malware can be determined by recording any associated activity on network connections, files and registries in Any.Run. Malware authors tend to test their skills by checking if their malicious code is running in the Any.Run malware analysis service or not.

US Government Shares Tips on Defending Against Cyberattacks

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

CISA issued protection guideline against cyberattacks routed through the Tor anonymity network. Tor is a software that automatically encrypt and reroute a user's web requests through a network of Tor nodes to enable anonymous communication. Malicious cyber actors can hide their identity and location by hiding real IP address while engaging in malicious cyber activity. Organisations should assess their individual risk of compromise via Tor and follow proper mitigation procedure to block or closely monitor inbound and outbound traffic from known Tor nodes. Organisations can use an indicator-based approach to detect malicious activity by looking for evidence of unusual traffic levels with Tor exit nodes in web server logs, packet capture and netflow.

Endpoint Protection Best Practices to Block Ransomware

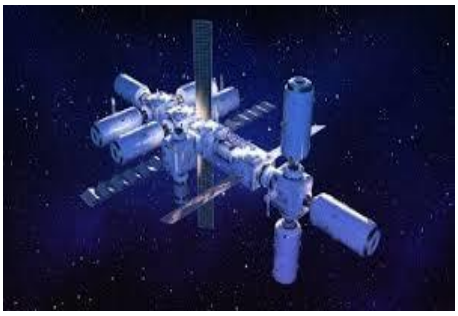
Source: *https://news.sophos.com/*

Most effective way of protecting against ransomware attacks like Maze, Sodinokibi, Ryuk and Ragnar Locker is to make sure that endpoint protection solution is properly configured. Some endpoint protection practices to block ransomware are:

- Turn on all policies and ensure that all features that detect file-less attack techniques and ransomware behaviour are enabled.
- Enabling multi-factor authentication provides extra layer of security.
- It is recommended to ensure all endpoints are protected and up to date. Endpoint detection and response (EDR) technologies can be used in endpoint solution to identify advanced threats and active adversaries, and take immediate action to stop threats.
- Maintain good IT hygiene to eliminate cyber security risk.
- Regularly review the exclusions. Excluded directories are more vulnerable to malware attacks.

How International Space Station Enables Cybersecurity

Source: https://www.hstoday.us/



The International Space Station (ISS) is also in potential cyber-risks like any other IT infrastructure. The space-based infrastructure including satellite is at risk even it is in space, from both physical and cyber-threats. Denial of service (DoS) which is basically blocking the signal is the simplest type of attack. The attacker can misconfigure a control system that eventually trigger a satellite to overheat or shutdown by intercepting and manipulating data transmission. Former NASA astronaut Pamela Melroy, outlined that the entire network by which NASA controllers at Mission Control communicate with ISS is a private network, operated by NASA. She also noted that there is a very rigorous certification process required for controllers in the International Space Station Mission Control Centre (MCC) to allow them to send commands to the space station and to limit the bad commands. In addition, there are also screening protocols both before a message leaves MCC going up to the

ISS and once it's on board ISS to prevent damage to the station.

DMARC Embraced by Government, Private Industry Lags

Source: https://www.scmagazine.com/

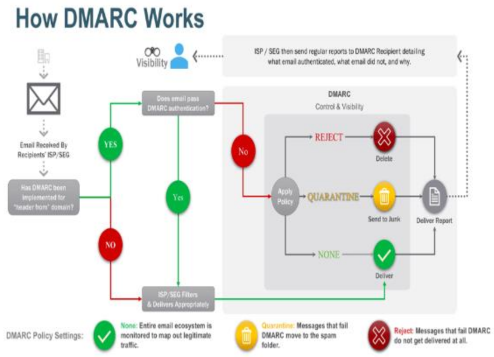

How DMARC Works
Visibility
ISP / SEG then send regular reports to DMARC Recipient detailing what email authenticated, what email did not, and why.
Email Received By Recipients' ISP/SEG
Has DMARC been implemented for "header from" domain?
YES
NO
Does email pass DMARC authentication?
Yes
No
ISP/SEG Filters & Delivers Appropriately
DMARC
Control & Visibility
Apply Policy
REJECT
QUARANTINE
NONE
Delete
Send to Junk
Deliver
Deliver Report
DMARC Policy Settings:
None: Entire email ecosystem is monitored to map out legitimate traffic.
Quarantine: Messages that fail DMARC move to the spam folder.
Reject: Messages that fail DMARC do not get delivered at all.

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

According to research by Valimail it has been found that 79% of Fortune 500 domains that can still be spoofed is because either no DMARC have been enforced, or they are using DMARC in "monitor mode," which ultimately doesn't protect an organisation from the attacks based on impersonation, even though the adoption of DMARC has grown over the past year. Among the eight private-sectors industry analysed, DMARC is enforced in 36% of large banks, up from 29% a year ago, and 21% of global banks are now protected by DMARC. In contrast, 19% of global tech companies and 10% of global media companies are DMARC-protected. Many of the domains which utilise DMARC but being used by spammers, phishers, and hackers for deception campaigns, but are not included in Valimail's analysis.

DNS Tunnelling and Fast Flux: Threat Hunting

Director, NSAC, NCIIPC

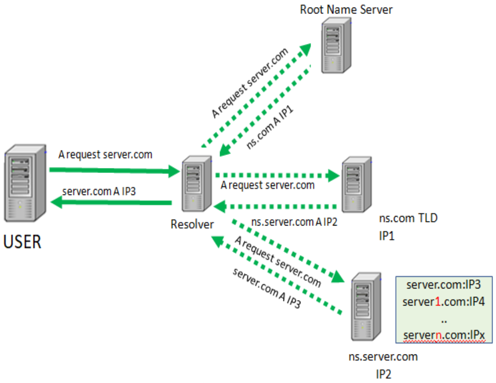


Figure 1

Domain Name System (DNS) process involves resolving the human readable domain name into corresponding IP addresses as the same are quite difficult to remember. DNS system is distributive system mentored by root name servers distributed across the globe and forms the essential component for effective functionality of the Internet. DNS system is divided in zones as per the domain categorisation. Entire request process for resolving the domain into IP goes broadly through several processes as highlighted in Figure 1 depending upon the availability of information at particular zone or locally in the DNS cache. DNS uses port 53 which is by default allowed in the network without much filtering rules available on firewalls. Moreover, DNS mostly relies on UDP protocol which is insecure by design; therefore, cyber criminals find it convenient to exploit the same. DNS is widely used and trusted as the same is not intended for data transfer; accordingly, it is also not monitored by majority of organisations giving motivation to malicious actors for exploiting the same for intruding and infiltrating/exfiltrating the data into/from the networks.

DNS Tunnelling and Fast Flux: DNS tunnelling attack is executed through encoding of data to be exfiltrated through DNS queries and responses. This is mostly undetected by firewalls as most of them are trusted being just the queries and response.

Through DNS tunnel attacker's C&C server interacts with the infected machine where the tunnelling program is usually installed. This communication forms the client-server model between the infected user and attacker's C&C. DNS domain generation/flux with Fast Flux basically involves in generating the flux of domains on victim machine along with malicious IP in command of attacker for additional payloads. Moreover, these malicious domains have small TTL value for resolution to particular IP due to which traditional way of blocking malicious IPs becomes ineffective. DNS domain with fast flux attack tunnelling process is highlighted in Figure 2.

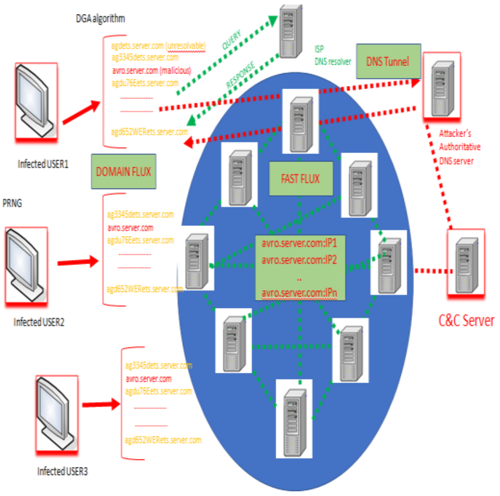


Figure 2

Threat Hunting: DNS monitoring and traffic analysis is vital component along with usual firewall traffic analysis considering the type of exploitations taking place in unmonitored DNS traffic as highlighted in above paragraphs. Some of the techniques in practice for identification of abnormality in DNS traffic are:

- Usually oversized request and response query through abnormal deviations in count of characters in FQDN and sub-domains.
- Looking for deviations in the usage of character combination, alphanumeric characters, and dictionary characters along with abrupt usage of special and encoded characters.
- Large forward DNS lookups of typo squatting.
- Queries to large non-existent domains through query failures.
- Abnormal amount of low TTL DNS beaconing queries.
- Large amount of uncommon query types viz. TXT records and PR, SOA AXFER queries for non-existent domains.
- Signature detection in the DNS traffic for available threat vectors.
- Abnormal volume of DNS generated by particular user in the network.
- Exceedingly high NXDomain responses for detecting DGA.
- Abnormal amount of DNS traffic attributed to particular domain only.
- Longer delays in HTTP response as a result of relaying request through Fast Flux (FF) domains.
- Abnormal DNS communication during off hours.
- Analysis of DNS queries to suspicious TLDs.

Countermeasures and Security Controls: Couple of security controls are highlighted to be in place for circumventing the DNS threats:

- DNS server should be configured to register both query and response traffic which should be thoroughly analysed for abnormality.
- Configuring and periodically compiling new Response Policy Zones (RPZ) used to block DNS queries and resolutions of known malicious actors.

DNS monitoring and traffic analysis is vital component along with usual firewall traffic analysis considering the type of exploitations taking place in unmonitored DNS traffic

- There should be limiting to DNS response rate.
- Restrict DNS zone transfer.
- Restrict DNS from being open resolver.
- Recommended to enable DNSSEC.
- All the Information disclosure of DNS should be blocked.
- In depth analysis and monitoring for threat hunting of any abnormality as highlighted above.

Conclusion: Since DNS is not on the priority list for hardening, filtering and monitoring by the security teams therefore bad actors have utilized DNS as a medium of C&C communication for exfiltrating the data from the network. Unusual DNS requests/response queries can be used by the Information Security/SOC Teams for threat hunting of DNS related abnormalities in the network. Separate DNS server with complete monitoring and enablement of DNSSEC is good security practices for avoiding the misuse of the same. Volumetric analysis of DNS in terms of abnormal amount of connections and data can be promising in identification of any suspicious usage apart from signature-based detection.

Since DNS is not on the priority list for hardening, filtering and monitoring by the security teams therefore bad actors have utilized DNS as a medium of C&C communication for exfiltrating the data from the network.

References:

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

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

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

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

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

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

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

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

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

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

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

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

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

Protocol Gateways

S&PE Sector, NCIIPC

A protocol gateway is a device that converts from one protocol to another which allows communication between various types of IT and OT devices that use different protocols. Let A and B be different protocols. In general, the typical structure of protocol gateway consists of a protocol-A slave, protocol-B master and an internal database. One scenario for a protocol gateway is the protocol-B master requests the remote protocol-B slave that communicates with devices, gets that device's data, and sends it to Protocol-B master which keeps it in the internal database. When protocol-A master such as a Programmable Logic Controller (PLC) asks the gateway for data, protocol-A slave obtains the data from the internal database, and sends it to remote protocol-A master. In another scenario the remote protocol-A master sends data or commands that are received by protocol-A slave. Protocol-A slave passes the data or command to protocol-B master, and requests protocol-B master to forward the data or command to the protocol-B slave which sends them to appropriate remote devices.

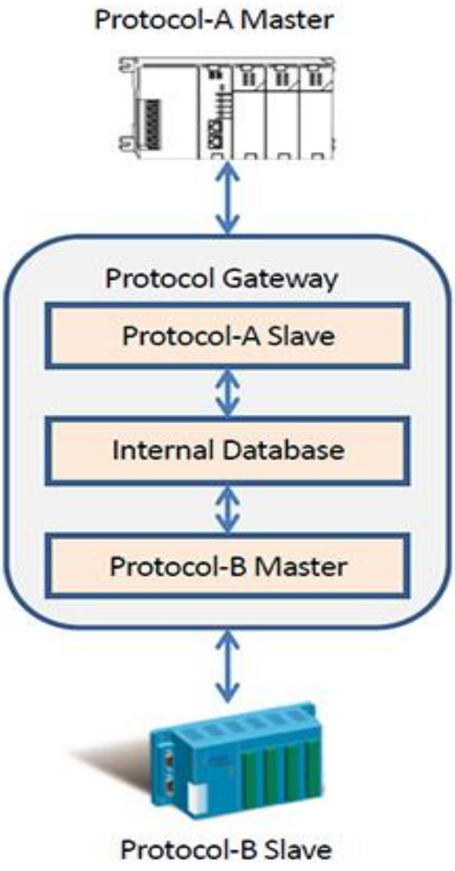


Figure 1: Typical Structure of a Protocol Gateway

Classification of Protocol Gateways:

Protocol gateways can be classified in to two types by the way they translate protocols.

- Realtime gateways: These gateways translate the incoming packets/data in real time according to the protocol specifications.
- Data Stations gateways: These types of gateways match the incoming packets/data using a translation table that the user is asked to configure in the gateway manually.

Protocol gateways can be classified in to three types by the type of protocols and layers they can translate.

- Translates different physical layers within a single protocol (e.g., Modbus TCP to Modbus RTU)
- Translates different protocols within a single physical layer (e.g., Modbus RTU to Profibus)
- Translates between different protocols as well as physical layers (e.g., Modbus TCP to Profibus)

Security risks and impact of using Protocol Gateways:

- If the protocol gateway fail, the communication between the control systems and the operating machines stop leading to disruptions in the operations and process.
- An attacker can target the protocol gateways through Denial of service by sending repeated commands or packets, manipulating of the I/O image and unauthorised commands.

An attacker can target the protocol gateways through Denial of service by sending repeated commands or packets, manipulating of the I/O image and unauthorised commands.

- This may lead to the Denial of view (preventing the operator from seeing the status of systems), Denial of control, manipulation of content to be viewed and manipulation of control.
- Researchers have analysed the Nexcom, Schneider, Digi One protocol gateways, which are used in many organizations. They have generated and sent invalid packets and commands to test the firewalling capabilities of these protocol gateways. Both the Schneider and Digi One devices filtered out most of the invalid packets, but the one from Nexcom has completely failed this test.

Since protocol gateways play a crucial role in industrial operations, security measures should be taken.

Securing Protocol Gateways: Since protocol gateways play a crucial role in industrial operations, security measures should be taken. Some of the strategies for protecting the protocol gateways are:

- Checking the filtering capabilities while procuring the devices.
- Consider a protocol-aware ICS firewall on the Control Network side and an in-house monitor on the process network side.
- Dedicating enough time to configure and secure the gateway.

References:

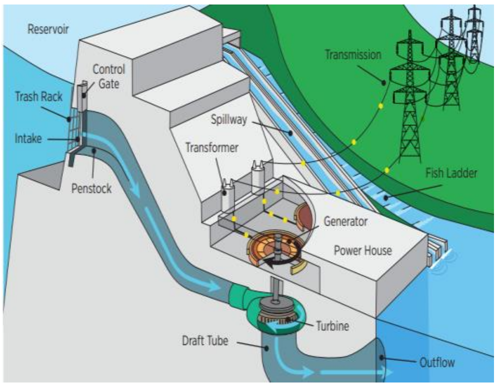
[1] https://www.trendmicro.com/vinfo/hk-en/security/definition/protocol-gateway/

[2] https://www.valin.com/resources/whitepapers/protocol-gateways-the-better-solution-for-protocol-conversion

[3] https://www.securityweek.com/vulnerabilities-protocol-gateways-can-facilitate-attacks-industrial-systems?&web_view=true

Hydro Power Generation: Cyber Threats

Power & Energy Sector, NCIIPC



Electricity supply begins with generation and relies on local control of output and wide-area control (Automatic Generation Control or AGC) of load and frequency. Local control loops which includes sensors/actuators that continuously provide data to control rooms that send commands to the generator equipment. Consequently, generation production is increased or decreased to meet generation demand conditions, and system load stability is balanced across all generation resources. It also does not depend on geographically distributed control systems and therefore a cyber-attack is considered more important on attaining access to the local control system. The hydro power has increased significantly in the past decade and leading to the adoption of innovative technology, advanced control systems (ICS/SCADA) and stronger equipment. When malicious attackers gain access to an industrial control system, they are able to disrupting industrial control and safety processes, leading to costly outages, damaged turbines, threats to personnel safety and even environmental disasters.

When malicious attackers gain access to an industrial control system, they are able to disrupting industrial control and safety processes, leading to costly outages, damaged turbines, threats to personnel safety and even environmental disasters.

Major Potential risk in Hydro Power generation:

- *Distributed Denial-of-Service (DDoS):* DDoS attack is another form of denial of service which involves disruption in network through a launched attack from many individual locations. Using botnets, cyber criminals can congest these exposed ICS devices with extra network traffic, thus overloading the devices and knocking them offline may result in some critical process prematurely halting, or the process could continue to run in an uncontrolled manner, causing severe material damage.
- *Vulnerability exploitation:* Vulnerability exploitation is the intentional exploitation of known impotencies in a software program in order to compromise the system, the end goal is almost always malicious. ICS devices have so many of publicly undisclosed vulnerabilities that an attacker can exploit in order to compromise the system.
- *Lateral movement:* In such type, a cyber-attack typically involves activities related to credential theft, reconnaissance, and infiltration of other system to target more critical devices or systems. Attackers compromise a machine inside the network, (here exposed ICS controller). In this way, an exposed ICS device could be the cause of a compromise to some backend database server also.

How can the Hydro generation power plant be secured?

Some important points to be considered while developing a security plan are:

- Industry needs to adopt cyber security best practices and develop a risk management culture.
- It is important to rapidly share information about cyber threats while respecting privacy guidelines.
- Good cyber security requires skilled teams to understand main root operations, detect and respond to abnormal cyber activity, reduce the "dwell time" of cyber attackers and implement layered cyber protection.
- There is a need to understand and increase system resilience to avoid prolonged outages and better recover from cyber-attacks.
- In the future, utilize advanced cyber security technologies, international approaches to cyber security, and machine-

It is important to rapidly share information about cyber threats while respecting privacy guidelines.

to-machine information sharing so the response to cyber incidents takes place in milliseconds—not months.

- Security Assessment: A thorough review of site infrastructure nuances, software, networks, control systems, policies, procedures, and even employee behaviours must be carried out at regular interval.
- Defense-in-Depth: Defense-in-depth (DiD) security is the idea that if any one point of protection is defeated, there are additional layers to protect the system that will need to be defeated for a hacking attempt to be successful. Defense-in-depth security approaches make multiple layers of protection by integration of physical, electronic, and procedural safeguards.
- Trusted Vendors: Before selecting vendors for any system that will be connected to network, request that they disclose their security policies and practices.

A thorough review of site infrastructure nuances, software, networks, control systems, policies, procedures, and even employee behaviours must be carried out at regular interval.

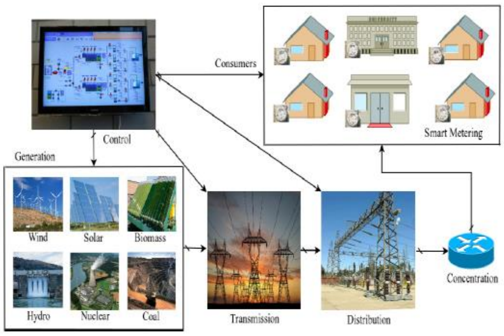
References:

[1] https://www.machinedesign.com/automation-iiot/article/21836539/how-to-protect-energy-plants-from-cyberattacks

[2] https://www.energy.gov/

Smart Grid Cyber Security: Threats and Security Solutions

Power & Energy Sector, NCIIPC



The smart grid is power grid in which electricity is managed and distributed through automation system. The segregation of advanced network, communications, and advanced techniques allows for improvement of efficiency and reliability. There are five factors to consider for efficient operation of the smart grid: communications, smart metering, distributed energy resources, monitoring and controlling.

Different types of Attacks in Smart Grid are:

- *Metering Infrastructure Attacks:* Meters can be hacked directly by reading diagnostic ports, accessing onboard memory and other network interfaces.
- *Jamming and Access Restriction:* In a jamming attack, attacker can prevent meters from connecting with utility company through stuffing wireless media with noise.
- *NAN Sniffing and Eavesdropping:* NAN sniffing is used to capture a smart meter's consumption data by breaking network encryption.
- *Energy Theft Attack:* An attacker can disrupt a

measurement before it takes place; one may fiddle with stored demand data either before or while the measurements are stored in meter; the adversary can modify the network even before or while the meter takes its data and logs it.

- *Fault Analysis Attack:* This class of attack can inject faults into a device performing some computation and checks the output signal to obtain patterns associated with encryption within the data.
- Denial of Service Attacks: This attack seeks to disrupt a power grid network by overwhelming its communication and computational resources in order to prevent it from working.
- Control and Monitoring Attacks: As many protocols lack authentication and are without encryption procedures. Thus, attacker can take the control of automation of Power system as well.

> *This attack seeks to disrupt a power grid network by overwhelming its communication and computational resources in order to prevent it from working.*

How can the Smart Grid be secured?

- Secure Key Management: Public key infrastructure being a standard for binding public cryptographic keys with user identities by means of central certificate authority and very useful when implemented as a key management device.
- Theft Detectors: A theft detector can be constructed by taking average of the series over a number of measurements and check whether this is less than some threshold value. This threshold value being the minimum of daily averages taken over a preset number of days in the past.
- Memory Attestation: Attestation refers to validating the integrity of a device for computing.
- Fault Analysis Countermeasures: The countermeasure against fault analysis attacks are (a) Sensor-based techniques which focus on finding environmental faults caused by such attacks and (b) Error-detection based strategies involve the introduction of redundancies at software, hardware and information levels in order to detect fault injection.
- SCADA Countermeasures: SCADA countermeasures includes Live Forensics, Industrial Protocol Filters and Intrusion Detection and Prevention Systems

> *A theft detector can be constructed by taking average of the series over a number of measurements and check whether this is less than some threshold value.*

References:

[1] https://www.academia.edu/33135231/

Vulnerability Watch

Critical Vulnerabilities in Treck TCP/ IP stack

Source: https://www.jsof-tech.com/ripple20/, https://www.tenable.com/

Multiple vulnerabilities dubbed as Ripple20 have been discovered in TCP/IP software library developed by Treck, Inc. Among which are the two critical vulnerabilities, i.e. CVE-2020-11896 and CVE-2020-11897 whose successful exploitation may lead to remote code execution and out-of-bound write respectively. These are caused by malformed packets being sent to a device that has IP tunneling enabled. The affected library exists in industrial devices, power grids, medical devices, networking devices, enterprise devices, and other IoT devices.

The impact of Ripple20 is magnified by the supply chain factor.

Critical Vulnerability in WebKitGTK and WPE WebKit

Source: https://nvd.nist.gov/, https://webkitgtk.org/security.html

Improper input validation vulnerability (CVE-2020-13753) has been discovered in WebKitGTK and WPE WebKit. The bubblewrap sandbox of the said products didn't properly block access to CLONE_NEWUSER and TIOCSTI ioctl. CLONE_NEWUSER which allows access outside the sandbox could be used to confuse xdg-desktop-portal and TIOCSTI could be used to directly execute commands outside the sandbox by writing to the controlling terminal's input buffer. It has a CVSSv3 Score of 10.0. Versions before 2.28.3 are affected. It is recommended to update to the latest stable versions.

The bubblewrap sandbox of the WebKitGTK and WPE WebKit products didn't properly block access to CLONE_NEWUSER and TIOCSTI ioctl.

Critical Vulnerability in SAP NetWeaver Application Server JAVA

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

Improper authentication vulnerability (CVE-2020-6287) also known as RECON (Remotely Exploitable Code On NetWeaver) has been discovered in SAP NetWeaver Application Server JAVA's LM Configuration Wizard. Affected versions are 7.30, 7.31, 7.40 and 7.50. It has a CVSSv3 Score of 10.0. Successful exploitation may allow an unauthenticated attacker to create a new SAP user with maximum privileges, bypassing all access and authorization controls and gaining full control of SAP systems. SAP has released security updates to mitigate the issue.

Successful exploitation may allow an unauthenticated attacker to create a new SAP user with maximum privileges.

Critical Vulnerability in Windows DNS Server

Source: https://portal.msrc.microsoft.com/, https://thehackernews.com/

Critical remote code execution vulnerability (CVE-2020-1350) dubbed as SigRed has been discovered in Windows DNS Server. The vulnerability is wormable and has a CVSSv3 Score of 10.0. Successful exploitation may allow an unauthenticated, remote attacker to gain domain administrator privileges over targeted servers. Windows Server versions 2003 to 2019 are affected. Microsoft has released update to address the vulnerability by modifying how Windows DNS servers handle requests.

The SigRed vulnerability is wormable and has a CVSSv3 Score of 10.0.

Critical Vulnerability in Oracle SD-WAN Aware and Edge

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

Insufficient information vulnerability has been discovered in Oracle SD-WAN Aware (CVE-2020-14701) version 8.2 and Oracle SD-WAN Edge (CVE-2020-14606) versions 8.2 and 9.0. It has a CVSSv3 Score of 10.0. Successful exploitation may allow an unauthenticated attacker with a network access via HTTP to compromise the affected product.

Critical Netlogon Elevation of Privilege Vulnerability

Source: https://portal.msrc.microsoft.com/

Elevation of privilege vulnerability (CVE-2020-1472) has been discovered in Netlogon. The vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller using the MS-NRPC. Successful exploitation may allow execution of a specially crafted application on a device on the network. It has a CVSSv3 Score of 10.0. The phase one update addresses the vulnerability by modifying how Netlogon handles the usage of Netlogon secure channels.

Successful exploitation may allow execution of a specially crafted application on a device on the network.

Attackers can Exploit Cisco Jabber Flaw with One Message

Threat Assessment, NCIIPC

Cyber security experts have warned against critical Remote Code Execution (RCE) flaw in Windows version of Cisco Jabber, the video-conferencing and instant-messaging application. Attackers can exploit the flaw simply by delivering targets specific crafted messages and user interaction is not required for this process. Currently this flaw is on target for attackers, in all types of organisations. Most of us are aware that sensitive data and information is shared through video calls or instant messaging system, and these various applications are used by majority of employees, including those who has privileged access to other IT Networks. An attacker can exploit these flaws by sending specially crafted Extensible Message and Presence Protocol (XMPP) messages to vulnerable end-user machine running on Cisco Jabber for Windows system. XMPP is an XML-based protocol for instant messaging used in both open-source as well as proprietary software. These attacks can be carried out remotely by access to the same XMPP domain or other method of access to be able to send messages to clients. This vulnerability can be exploited also when Cisco Jabber application is running in background of any windows machine. The problem originates from Cisco Jabber application as it does not properly sanitize incoming HTML messages and simply passes the messages through a flawed cross-site scripting (XSS) filter which can be bypassed by using an attribute known as onanimationstart. This attribute is used to define a JavaScript function which will be called when an element's CSS animation starts playing. Using this attribute, it is possible to create malicious HTML tags which filter did not identify and ultimately executed. Finally, attackers are able to create a malicious message by using these HTML tags, which also intercept an XMPP message sent by application and modify that. Computer Systems using Cisco Jabber in phone-only mode (without XMPP messaging services enabled) are not vulnerable to this exploitation, Also, this vulnerability is not exploitable when Cisco Jabber is configured to use messaging services other than XMPP messaging. The vulnerability affects all current versions of the Cisco Jabber client (12.1 – 12.9). Cisco has released updates for affected versions of Cisco Jabber.

The problem originates from Cisco Jabber application as it does not properly sanitize incoming HTML messages and simply passes the messages through a flawed cross-site scripting (XSS) filter which can be bypassed by using an attribute known as onanimationstart.

References:

[1] https://threatpost.com/

Cisco Patches Critical Vulnerability in DCNM

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

Critical authentication bypass vulnerability (CVE-2020-3382) has been discovered in the REST API of Cisco Data Center Network Manager (DCNM). The vulnerability exists due to static encryption key shared by different installations. This static key could be used by an attacker to craft a valid session token. Successful exploitation may allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected device. Affected versions of Cisco DCNM software are 11.0(1), 11.1(1), 11.2(1), and 11.3(1). Cisco has released software updates to fix this vulnerability.

Affected versions of Cisco DCNM software are 11.0(1), 11.1(1), 11.2(1), and 11.3(1).

Critical Vulnerabilities in Industrial VPN Implementations

Source: https://thehackernews.com/

Critical vulnerabilities CVE-2020-14500, CVE-2020-14511 and CVE-2020-14498 have been discovered in Secomea's GateManager, Moxa's EDR-G902, and EDR-G903, and HMS Networks' eCatcher respectively. These vulnerable products are widely used in field-based industries such as oil and gas, electric utilities, and water utilities to remotely access, maintain and monitor ICS and field devices, including programmable logic controllers (PLCs) and input/output devices. Successful exploitation could allow an attacker to overwrite data, execute malicious code, and compromise industrial control systems. All the vendors have released software updates to address respective vulnerabilities.

Successful exploitation could allow an attacker to overwrite data, execute malicious code, and compromise industrial control systems (ICS).

Vulnerability in OSIsoft PI System can Facilitate Attacks on CI

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

Stored XSS vulnerability (CVE-2020-12021) has been discovered in the PI Web API 2019 component of OSIsoft PI System. Version 1.12.0.6346 and prior are affected by this flaw. Successful exploitation may allow a remote authenticated attacker with write access to a PI Server to trick a user into interacting with a PI Web API endpoint that executes arbitrary JavaScript in user's browser, resulting in view, modification, or deletion of data as allowed for by victim's user permissions.

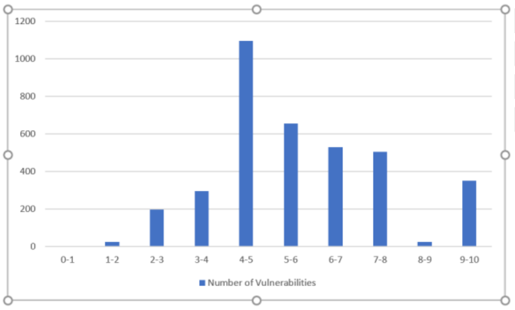
In order to exploit this vulnerability an external attacker needs to gain access to the PI Server.

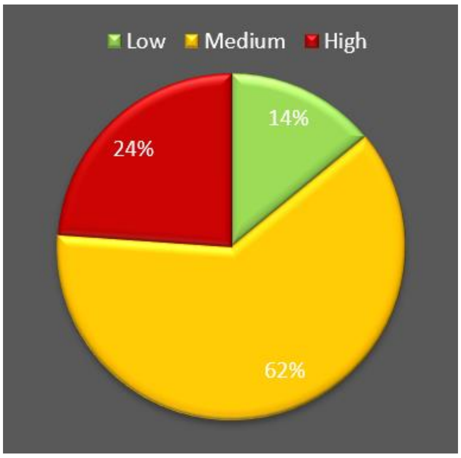
Quarterly Vulnerability Analysis Report

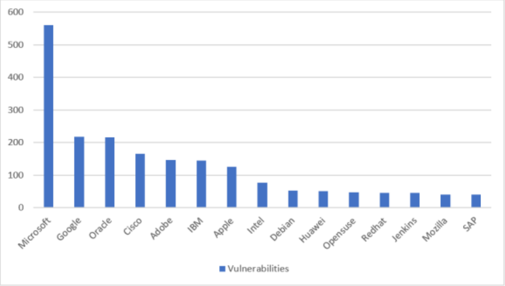
KMS Team, NCIIPC

A total of 3671 vulnerabilities have been observed in the month of Jun - Aug 2020. Most of the vulnerabilities had a score ranging from 4-7. 62 percent of total vulnerabilities reported were of medium severity. Microsoft, Google, Oracle, Cisco and Adobe were the top five vendors.

Severity	CVSS Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Jun	Jul	Aug		
Low	0-1	0	0	0	0	514
	1-2	6	14	4	24	
	2-3	82	57	57	196	
	3-4	125	103	66	294	
Medium	4-5	389	423	283	1095	2280
	5-6	290	244	122	656	
	6-7	219	182	128	529	
High	7-8	214	180	109	503	877
	8-9	9	9	6	24	
	9-10	160	119	71	350	
Total		1494	1331	846		3671







Vendor	No. of Vulnerabilities			Total
	Jun	Jul	Aug	
Microsoft	224	166	170	560
Google	140	50	27	217
Oracle	2	213	0	215
Cisco	90	50	25	165
Adobe	96	23	28	147
IBM	53	47	45	145
Apple	94	3	28	125
Intel	26	0	50	76
Debian	26	17	9	52
Huawei	12	23	16	51
Opensuse	25	14	8	47
Redhat	14	17	15	46
Jenkins	11	26	9	46
Mozilla	1	25	15	41
SAP	13	14	13	40

Security App

REMnux: A Linux-based Malware Analysis Toolkit

Source: https://gbhackers.com/remnuxv7/

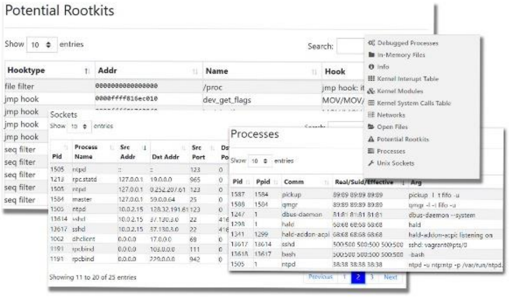
REMnux is a linux distro toolkit for reverse-engineering and analysing malicious software. A new version of REMnux Linux distro has been released for malware researchers. The new version is packed with hundreds of tools to dissect malicious executables, scripts, documents, and ill-intended code. This new REMnux release is fully rebuilt and it relies on SaltStack to automate the installation and configuration of software, thereby allowing community members to contribute with tools and revisions.

> *The REMnux utilities are configured in a particular way to help reverse engineers save time and get to analysing malware faster.*

Microsoft Linux Forensics and Rootkit Malware Detection Service

Source: https://thehackernews.com/

Microsoft announced a new free tool for uncovering forensic evidence of sabotage on Linux systems, which includes intrusive malware and rootkits that normally go undetected. This tool is called Project Freta, it is a snapshot-based memory forensic technique. Project Freta has the ability to spot kernel rootkits, malicious software, and other stealthy malware techniques. The main objective of this project is to infer the presence of malware from memory, at the same time gain an upper hand against threat actors who deploy and reuse stealthy malware on target systems for ulterior motives. This tool works on four aspects that would make



Potential Rootkits

Show 10 entries Search:

Hooktype	Addr	Name	Hook
file filter	0000000000000000	/proc	jmp hook: it
jmp hook	0000ffff816ec010	dev_get_flags	MOV/MOV/
jmp hook			
jmp hook			
jmp hook			
seq filter			
seq filter			
seq filter			
seq filter			
seq filter			

Sockets

Show 10 entries

Pid	Process Name	Src Addr	Dst Addr	Src Port	Ds Po
1505	ntpd	::	::	123	0
1213	rpc.statd	127.0.0.1	19.0.0.0	965	0
1505	ntpd	127.0.0.1	0.252.207.61	123	0
1584	master	127.0.0.1	59.0.0.64	25	0
1505	ntpd	10.0.2.15	128.32.191.61	123	0
13614	sshd	10.0.2.15	37.130.3.0	22	416
13617	sshd	10.0.2.15	37.130.3.0	22	416
1062	dhclient	0.0.0.0	17.0.0.0	68	0
1191	rpcbind	0.0.0.0	103.0.0.0	111	0
1191	rpcbind	0.0.0.0	229.0.0.0	942	0

Showing 11 to 20 of 25 entries

Processes

Show 10 entries

Pid	Ppid	Comm	Real/Suid/Effective	Arg
1587	1584	pickup	89:89 89:89 89:89	pickup -l -t fifo -u
1588	1584	qmgr	89:89 89:89 89:89	qmgr -l -t fifo -u
1247	1	dbus-daemon	81:81 81:81 81:81	dbus-daemon --system
1298	1	hald	68:68 68:68 68:68	hald
1341	1299	hald-addon-acpi	68:68 68:68 68:68	hald-addon-acpi: listening on
13617	13614	sshd	500:500 500:500 500:500	sshd: vagrant@pts/0
13618	13617	bash	500:500 500:500 500:500	-bash
1505	1	ntpd	38:38 38:38 38:38	ntpd -u ntp:ntp -p /var/run/ntpd.

systems immune to such attacks by preventing any program from:

- Prior installing itself it detects the presence of a security sensor.
- It resides in an area that is out of the sensor view.
- Detecting the sensor's operation and accordingly erasing or modifying itself to escape detection.
- Tampering with the sensor's functions to cause sabotage.

Project Freta lets users submit memory images (.lime, .vrms, .core, or .raw files) via an online portal or an API.

Project Freta has the ability to spot kernel rootkits, malicious software, and other stealthy malware techniques.

Pysa: Facebook Open Source Security Analysis Tool

Source: https://latesthackingnews.com/

Facebook released Pysa, a security tool internally developed by Facebook based on open-source code of Pyre project. Pysa has been developed as a static code analyser. The tool specifically searches for security bugs, unlike most other analysers. Pysa also detects common web app security issues, like XSS and SQL injection. It is designed to track the flow of data through a program. This tool helps in analysing huge codebases with millions of lines of codes. It can build summaries by repeatedly analysing the functions and noting whether the return data comes from source (point of origin of important data) or the sink (points where source data should not end).

This tool helps in analysing huge codebases with millions of lines of codes.

Stringlifier: Adobe Open Source Security Tool

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

Adobe has released an open source tool Stringlifier that identifies any randomly generated strings in any plain text. This tool has been written in Python and leverages machine learning to differentiate random character sequences from normal text sequences. This tool also proves to be helpful when analysing security and application logs, or when looking for credentials that might have been accidentally exposed. Adobe has already used the tool for detecting random strings when looking for anomalies in datasets.

BlackBerry Releases Open Source Reverse Engineering Tool

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

BlackBerry has released a new open source tool named PE Tree to help security teams reverse engineer malware. With help of PE Tree the reverse engineers can view the Portable Executable (PE) files in a tree-view using PyQt5 and pefile, thereby lowering bar for dumping and reconstructing malware from memory. PE Tree can also be integrated with Hex-Rays' IDA Pro decompiler to allow for simple navigation of PE structures, as well as

dumping in-memory PE files and performing import reconstruction; critical in the fight to identify and stop various strains of malware. PE Tree has been developed using in Python, it supports Windows, Linux, and macOS systems, and can be installed and run as either a standalone application or an IDAPython plugin.

AutoGaDgetFS Lets Users to Assess Their USB Devices

Source: https://agfs.io/#About

AutoGadgetFS is an open source framework that lets users to assess their USB devices and associated hosts/drivers/software without an in-depth knowledge of USB protocol. AutoGadgetFS is written in Python3 and it utilizes RabbitMQ and WiFi access to let researchers conduct remote USB security assessments from anywhere around the world. By leveraging ConfigFS, AutoGadgetFS allow users to clone and emulate devices quickly, eliminating the need to dig deep into details of each implementation. The framework also allows users to create their own fuzzers on top of it.

By leveraging ConfigFS, AutoGadgetFS allows users to clone and emulate devices quickly, eliminating the need to dig deep into the details of each implementation.

vPrioritizer

Source: https://www.blackhat.com/

vPrioritizer is a tool that provides the ability to assess the risk on different layers and thereby provides control on granularity of each component of risk. This framework enables user to understand the contextualized risk regarding each asset by each vulnerability across the organization. It's community-based analytics and provides a suggested risk for each vulnerability identified by vulnerability scanners and further strengthens risk prioritization process. So, at any point of time teams can make an effective and more informed decision, based on unified and standardized data, about what vulnerability they should remediate or if possible, not to on which asset.

This framework enables user to understand the contextualized risk regarding each asset by each vulnerability across the organization.

Mobile Security

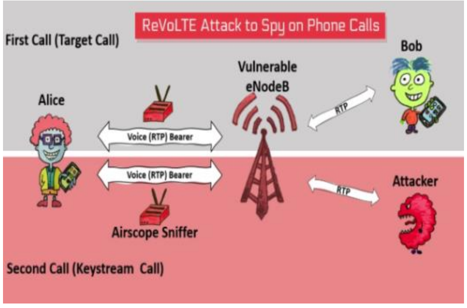
Vulnerability in Encrypted Voice Calls on VoLTE networks

Source: https://thehackernews.com

A new attack vector has surfaced which could eavesdrop on encrypted phone calls made on VoLTE (Voice over Long Term Evolution protocol) networks. Termed as ReVoLTE, it takes advantage of the same keystream used to encrypt voice data in subsequent phone calls. Here an attacker records phone calls of his victim by placing a downlink sniffer in the same base station of his victim's voice call. Within 10 seconds of hanging up, the attacker calls his victim and takes advantage of the vulnerable network and records his voice call data in plain text

A new attack vector has surfaced which could eavesdrop on encrypted phone calls made on VoLTE (Voice over Long Term Evolution protocol) networks.

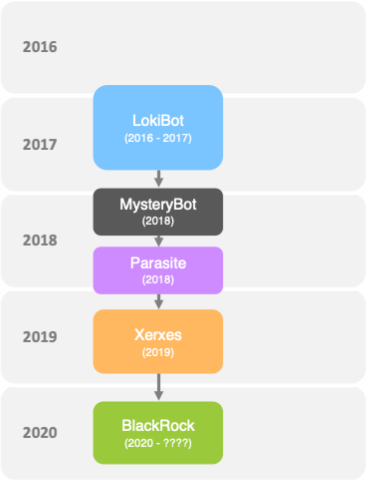
from which attacker reverse computes the keystream used to encrypt the previous voice call. The previous encrypted call can now be easily decrypted by XOR-ing the keystream and encrypted frames. The attack has also been demonstrated by academics at Ruhr University Bochum using downlink analyser Airscope by Software Radio System. They have also released an open source Android app named 'Mobile Sentinel', which can be used to detect this type of attack.



BlackRock: from the family of Xerxes Banking Malware

Source: https://www.threatfabric.com/blogs/

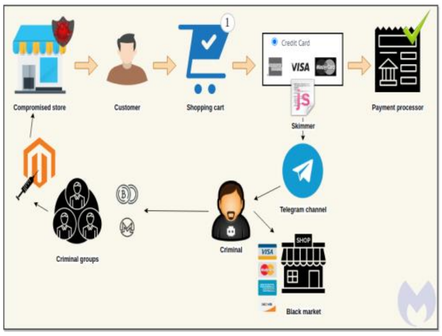
A new malware termed as BlackRock, based on code of famous Xerxes banking malware is found to be targeting a unique list of 337 popular online socializing apps. Some of the features of BlackRock include performing overlaying attacks, abusing SMS messages, locking the victim out of its device and acting as a keylogger. After installation, the malware hides its icon and asks for Accessibility Service privilege by posing itself as fake Google update. For the threat of being removed, the malware redirects its victim to the home screen of the device whenever he/ she tries to open an antivirus app. The malware uses local files as overlays which are downloaded on the infected device beforehand for stealing credentials of banking applications.



Web Skimming Using Telegram

Source: https://blog.malwarebytes.com

Online shopping websites are always under the threat of web skimmers. A new threat has been discovered in which stolen credit card details are being stored in private Telegram channels. Whenever a user lands on payment page of a compromised website, the skimmer extracts user's personal and banking information and sends it to a private Telegram channel using Telegram bot ID and channel via Telegram API request where the requests are encoded in base64 to avoid detection. This attack requires fewer infrastructures and is harder to track. Also, the attacker gets his victims payment details in real time.



Joker Malware Plagues Six More Google Play Apps

Telecom Sector, NCIIPC

Joker is a trojan malware and is activated only when a user interacts with the malicious app installation. The virus then goes into the device's security options and is in a position to render the device useless or steal the information. It is affected by downloading a secured configuration from a Command-and-Control (C&C) server within variety of app-installations. The

hidden software then installs a follow-up software or applications that steal SMS details without user's interaction. It also steals money from users by enabling apps to premium services without user permissions. Authentications like OTPs are obtained by stealing SMS information. In this regard, Google has strict preventive measures in place to check for this type of malwares. Earlier, Google has removed more than 1,700 apps infected with Joker malware from Google Play and now new apps have been found by researchers of different cybersecurity organisations. Recently, six new apps on Google Play were identified by cybersecurity researchers as having been infected with joker malware. These apps had more than 2 lakh downloads in total. The six apps are:

- Convenient Scanner 2 (Version: 14.0.4) has been downloaded more than 100,000 times.
- Separate Doc Scanner (Version: 2.0.74) has been downloaded by 50,000 users.
- Safety AppLock (Version: 6.5) claims to protect privacy and has been installed 10,000 times.
- Two apps have received 10,000 downloads each – Push Message-Texting & SMS (Version: 4.13) and Emoji Wallpaper (Version: 14.3).
- Fingertip GameBox (Version: 3.0.7) has been downloaded 1,000 times.

Joker malware infected apps are deleted from Google Play However, still installed on the devices of their users. Users are advised to immediately delete the apps from device to avoid fraudulent or miscellaneous activities.

References:

[1] https://www.zdnet.com/article/android-security-six-more-apps-containing-joker-malware-removed-from-the-google-play-store

[2] https://www.theweek.in/news/sci-tech/2020/07/13/What-is-the-Joker-malware-Heres-how-it-affects-apps.html

[3] https://blog.pradeo.com/pradeo-identifies-app-joker-malware-google-play

NCIIPC Initiatives

IEEMA Workshop on Cybersecurity

IEEMA (Indian Electrical and Electronics Manufacturers' Association) organised a workshop on cybersecurity on 6 Aug 2020. It witnessed participation from across the industry and utilities. During this workshop IEEMA also launched its Whitepaper on cybersecurity imperative for Indian Electricity infrastructure. It was followed by a Panel Discussion on 'Building Resilient Electrical Infrastructure-under constant threat of Cyber-attacks' with panelists: Mr. MAKP Singh, CE (IT), Central Electricity Authority; Mr. A.K Mishra, Director, NSGM; Mr. Lokesh Garg, DDG, NCIIPC & Mr. Ganesh Srinivasan, CEO, Tata Power – DDL.

Participants of IEEM virtual conference

Webinar on Information Security Management Systems

NCIIPC along with M/s Ernst & Young (E&Y) organised a webinar on Information Security Management Systems Framework (ISMSF) for Critical Sectors on 14 Aug 2020. Sh. Abhijeet Raj Shrivastava, Director (Power & Energy) presented about Roles of National Critical Information Infrastructure Protection Centre. The Webinar was attended by more than 200 participants from about 50 organisations.

Webinar was attended by more than 200 participants from about 50 organisations.

NCIIPC's Participation at Government of West Bengal's Webinar

A webinar was organized by Department of IT and Electronics, Government of West Bengal for resources, registered in Karmo-Bhumi Skill Registry Platform (https://karmobhumi.nltr.org) under the category of Cyber Security. It was held on 18th September 2020 over a virtual platform. Sh. Rajeev Kumar, IPS, Principal Secretary, Dept of IT&E, Govt of West Bengal inaugurated the webinar. Smt. Smita Pandey, IAS, Managing Director, M/s WBEIDC Limited and Dr. Nabarun Bhattacharya, Director, C-DAC Kolkata graced the webinar too. Shri Tathagata Datta of NCIIPC, took part in the panel discussion alongside co-panelists Sh. Deb Kumar Roy from Cognizant and Sh. Sushobhan Mukherjee from InfoSec Foundation. Sh. Asok Bandopadhyay from C-DAC Kolkata moderated the panel discussion. During discussions, Sh. Datta talked about the required skills to protect National Critical Infrastructure, emerging threats and mitigation by application of technology and robust processes.

Participants of Govt of West Bengal's webinar

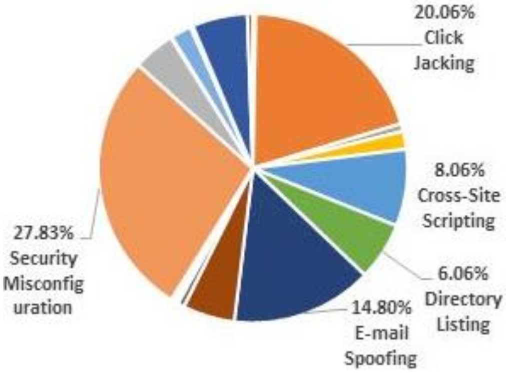
A webinar was organized by the Department of IT and Electronics of Govt of West Bengal for the resources, registered in Karmo-Bhumi Skill Registry Platform of Govt of WB, under the category of Cyber Security.

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. A total of 1750 vulnerabilities were reported during 11 Jun - 10 Sep 2020. Following are the top 10 vulnerabilities:

- Security Misconfiguration
- Click Jacking
- E-mail Spoofing
- Cross-Site Scripting
- Directory Listing
- Weak Cipher
- Injection
- Sensitive Data Exposure



- User Enumeration
- Cross-Site Request Forgery (CSRF)

Around 367 researchers contributed in this program. NCIIPC acknowledges following top 15 researchers for their contributions for protection of National Critical Information Infrastructure:

- Sachin Mishra
- Pratik Chotaliya
- Navaneeth Shyam
- Isa Ghojaria
- Darksteel Bughunter
- rjdpbsu@gmail.com
- Santosh Kumar
- Vidhi Waghela
- Dhiraj Vijyakumar Ramteke
- Pankaj Kumar Thakur
- K.V.S Mani Kumar
- Priyank Parmar
- Mahammed Aashique
- Shashwat
- Hemant Patidar

On the Fly

Zhenhua Data Leak

Source: https://en.wikipedia.org/wiki/Zhenhua_Data_leak

A data leak in Zhenhua revealed that it had been monitoring over 2.4 million people globally. The databases of Zhenhua, collectively known as Overseas Key Information Database (OKIDB), was leaked to an American academic who shared these data with Internet 2.0, an Australian based cybersecurity consultancy, for recovery and analysis. Researchers discovered that about 20% of data in Zhenhua was not from open source locations. Investigation had also found that some person with no online presence have also been profiled in database. Internet 2.0 recovered a quarter of a million people from OKIDB, including about 52,000 Americans, 10,000 British, and 35,000 Australians were being observed by Zhenhua. Around 10,000 people and many organisations from India were also on the list. Numerous Indian think-tanks were also being monitored. Zhenhua also performed real-time monitoring of social media such as Facebook, TikTok, LinkedIn, Twitter and online forums. In-addition to these data sources Zhenhua also seem to have private sources of data on real-time movement of satellite tracking, warships, troop movements, etc.

Researchers discovered that about 20% of the data in Zhenhua was not from open source locations.

Upcoming Events - Global

October 2020

• Oil & Gas Cybersecurity Summit 2020	2 Oct
• Critical Infrastructure Protection & Resilience Europe, Bucharest	6-8 Oct
• Cyber Security for Critical Assets Europe, London	6-7 Oct
• Florida Cyber Conference, Orlando	8-9 Oct
• SecTor Canada, Toronto	19-22 Oct
• Workshop on Cyber Security and Resilience in the Internet of Things, Beijing	19-23 Oct
• International Workshop on Security, Privacy, and Trust for Emergency Events, Washigton DC	20 Oct
• BSides Ecuador 2020, Ecuador	22 Oct

November 2020

• BSides Tokyo 2020, Tokyo	1 Nov
• SANS DFIRCON 2020, Virtual	2-7 Nov
• New Jersey Cyber Security Conference, Virtual	5 Nov
• Great Lakes Virtual Cybersecurity Conference,	5 Nov
• Black Alps Cyber Security Conference, Yverdon les Bains	5-6 Nov
• Black Hat Europe 2020, London	9-12 Nov
• DEEPSEC, Vienna	17-20 Nov
• European Interdisciplinary Cybersecurity Conference, Rennes	18-19 Nov
• Paranoia, Osla	23-25 Nov

December 2020

• Cybersecurity & Fraud Summit: Seattle, Virtual	1 Dec
• San Diego Cybersecurity Conference	2 Dec
• FutureCon Denver CyberSecurity Conference	3 Dec
• IEEE Global Conference on Artificial Intelligence and Internet of Things, Dubai	12-15 Dec
• International Conference on Cryptology And Network Security, Vienna	14-16 Dec
• FutureCon Virtual Eastern Conference	15-18 Dec
• International Conference on Advanced Computing and Intelligent Engineering, Dubai	28-29 Dec

OCTOBER 2020

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

NOVEMBER 2020

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					

CYBER SECURITY FOR CRITICAL ASSETS | EUROPE

FutureCon Your CyberSecurity Conference HQ

DECEMBER 2020

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

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

January 2021

• FloCon 2021, Santa Fe	11-14 Jan
• CRESTCon UK 2021, London	13 Jan
• 13th International Conference on Global Security, Safety & Sustainability	14-15 Jan
• FutureCon Detroit Cyber Security Conference	20 Jan
• Cyber Security for Critical Assets MENA, Dubai	25-26 Jan
• IT-Defense 2021, Berlin	27-29 Jan
• FutureCon San Diego Cyber Security Conference	28 Jan

Upcoming Events - India

• Virtual Conference on Industry 4.0, Chennai	2-3 Oct
• BSides Ahmedabad, Ahmedabad	24 Oct
• Yet Another Security Conference, Kerala	1 Nov
• Virtual Cybersecurity Summit, Bengaluru	26 Nov
• IoT and Intelligent App, Chennai	4 Dec
• 21st International Conference on Cryptology in India, Bengaluru	13-16 Dec
• Cybersecurity Summit, Mumbai	15 Dec
• 10th International Conference on Security, Privacy and Applied Cryptographic Engineering, Kolkata	17-21 Dec

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

National Critical Information Infrastructure Protection Centre

सत्यमेव जयते

NCIIPC

सम्पूर्ण सुरक्षा

A unit of NTRO

Feedback/Contribution

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

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