NEWSLETTER

October 2018

National Critical Information Infrastructure Protection Centre

VOLUME 2 ISSUE 4

@NCIIPC

NCIIPC Newsletter

October 2018

Inside This Issue

Cybercriminals are targeting smaller banks with weaker security implementations. Nations need to come together to successfully counter such type of global threats.

Message from the NCIIPC Desk

In the previous months we observed new varieties of sophisticated threats emerging worldwide in banking sector. India, too, witnessed the heat where attackers successfully used the vulnerabilities of different systems at multiple levels and compromised them in a coherent way to siphon out millions in various transactions across the globe.

Cybercriminals are targeting smaller banks with weaker security implementations. Nations need to come together to successfully counter such type of global threats. Indian Banks Association has called for Cyber Security Insurance Cover for banks to cover the losses due to cyber-attacks. RBI has also issued strict directives to Indian banks to implement various security controls for the ATMs by June 2019. One of the controls is of upgradation of the unsupported operating systems like Windows XP. This will pave the way for implementation of advanced controls to counter emerging sophisticated threats.

Two Information Security Awareness Workshops on Protection of Critical Information Infrastructure were organised by NCIIPC at Chandigarh. The first was for the officers of Haryana State and the second designed for the senior officers of Punjab Police. NCIIPC has also established a Cyber Security Training Centre at Dehradun for Government of Uttarakhand.

NCIIPC encourages engagement with interns, cyber security professionals and researchers through various initiatives, details of which are available on NCIIPC web portal. Contribution of various researchers in reporting the prevalent vulnerabilities in Indian Critical Information Infrastructure is invaluable towards ensuring its safety, security and resilience.

NCIIPC conveys the very best wishes to all its stakeholders on the upcoming festivals of Navratri, Dussehra, and Deepawali.

Please do provide your feedback. For subscription, contribution or suggestions please write to us on newsletter@nciipc.gov.in.

News Snippets - National

Maharashtra shuts down Websites providing Pirated Contents

Source: https://www.indiatoday.in/

Maharashtra Cyber Digital Crime Unit (MCDCU) has shut down 29 websites providing pirated copies of Bollywood, Hollywood and TV content since a long time. It started as a pilot project in order to protect intellectual property from piracy and is being termed as first of its kind initiative in South Asia. An estimated 88.56 million users were found to be using the suspended websites. These were amongst the most sought-after websites being surfed for pirated content. MCDCU issued notices to the concerned domain registrars under Section 149 of Criminal Procedure Code forcing them to suspend operations of these websites.

MCDCU issued notices to the concerned domain registrars under Section 149 of Criminal Procedure Code forcing them to suspend operations of these websites.

Banks to Implement Security Controls for the ATMs by June 2019

Source: https://www.rbi.org.in/

The slow progress on part of the banks in addressing security issues has been viewed seriously by the Reserve Bank of India (RBI). RBI in a notification to all banks has suggested certain control measures for the ATMs for implementation by all banks in a phased manner by June 2019. Some of the control measures are:

- Implementation of BIOS password, disabling USB ports, disabling auto-run facility, applying the latest patches of operating system and other software, terminal security solution, time-based admin access, etc.
- Anti-skimming and whitelisting solution.
- Upgrade all the ATMs with supported versions of operating system.

Any deficiency in timely and effective compliance of the instructions may invite appropriate supervisory enforcement action.

Upgrade all the ATMs with supported versions of operating system.

Kerala to set up a State-of-the-Art Security Operations Centre

Source: http://www.newindianexpress.com

In the wake of repeated attacks on government websites in the past few years, Kerala State IT Mission has decided to set up a state-of-the-art Security Operations Centre (SOC) at a cost ranging from Rs. 5-7 crore. The SOC will be equipped to monitor and analyse activity on networks, servers, endpoints, databases, applications, websites and other systems. It will look for anomalous activity that could be indicative of a security incident or compromise. It will act as a pre-emptive centre to resist a cyber-attack.

It will look for anomalous activity that could be indicative of a security incident or compromise.

Indian Banks Association asks Banks to buy Cyber Insurance

Source: https://timesofindia.indiatimes.com

Cyber cover provides protection against multiple threats, such as loss caused by cyber heists, customer claims following a data breach, and cost of ransom payment in case of ransomware attack.

The Indian Banks Association has asked member banks to buy cyber insurance covers in the wake of several incidents of digital attacks on lenders. Cyber cover provides protection against multiple threats, such as loss caused by cyber heists, customer claims following a data breach, and cost of ransom payment in case of ransomware attack. The cyber liability policy would also cover loss of business due to a shutdown following a suspected malware attack. ICICI Lombard chief of underwriting, reinsurance and claims, Mr. Sanjay Datta said banks have to first take all required steps to protect themselves. The safety features include having necessary firewalls in place and adopting best practices.

Cosmos Bank Cyberattack

Source: https://www.zdnet.com

Threat actors failed in their first attempt to compromise the bank's systems, but no alert was issued to put the bank on guard against suspicious activity.

Cosmos Bank, one of the oldest Urban Co-operative Banks in India, became the victim of a cyberattack which left the institution millions out of pocket. The attack took place in two stages in-between August 10 - 13. The first wave involved the theft of roughly $11.5 million in transactions from multiple countries. In the second wave, on the same day, close to $2 million was withdrawn through debit card transactions across India. Funds were later transferred to Hong Kong through fraudulent SWIFT transactions. Cosmos Bank chairman Mr. Milind Kale said the cyberattack was a global effort as cyber attackers operated from 22 countries. Reports suggest that the threat actors failed in their first attempt to compromise the bank's systems, but no alert was issued to put the bank on guard against suspicious activity. According to Securonix Threat Research team, malware was used in tandem with an infected central ATM or POS switch. When the first stage of the attack was implemented, the malware likely severed the connection between central systems and the backend core banking system to prevent transaction verification.

News Snippets - International

Cyberattack on Singapore's Government Health Database

Source: https://www.bbc.co.uk/

Computer belonging to SingHealth, one of the state's two major government healthcare groups, was infected with malware through which the hackers gained access to the database.

A major cyber-attack on Singapore's government health database stole personal information of about 1.5 million people, including its Prime Minister. Computer belonging to SingHealth, one of the state's two major government healthcare groups, was infected with malware through which the hackers gained access to the database. They struck between 27 June and 4 July, according to the government.

Banco de Chile, Chile's largest Bank Hit by Cyber Attack

Source: https://www.theregister.co.uk

Chile's largest bank Banco de Chile was hit on 24 May and thousands of workstations hobbled. Banco de Chile's CEO, Eduardo Ebensperger Orrego, told that the attackers stole $10m from bank. Bank disabled 9,000 workstations to stop the virus's spread before spotting 'unusual transactions' on the bank's local SWIFT network. Hackers reportedly used a variant of the complex KillDisk wiper malware to distract attention before targeting systems linked to the SWIFT inter-bank transfer network. The assault followed the same pattern as the recent unsuccessful attack that trashed computers at a Mexican Bank but didn't result into any financial losses.

Computer screen of an infected computer in Bank's office (https://badcyber.com)

US moves to Block China Mobile from offering Services

Source: https://www.cnbc.com

The U.S. government moved to block China Mobile from offering services to the U.S. telecommunications market, recommending its application be rejected because the government-owned firm posed national security risks. National Telecommunications and Information Administration said the company was "subject to exploitation, influence and control by the Chinese government" and that its application posed "substantial and unacceptable national security and law enforcement risks in the current national security environment".

Its application posed "substantial and unacceptable national security and law enforcement risks in the current national security environment".

Ukraine Thwarted VPNFilter Attack on Chlorine Plant

Source: https://www.theregister.co.uk

Ukraine's SBU Security Service claimed that it thwarted a VPN Filter malware attack on network equipment belonging to the LLC Aulska chlorine plant. "Specialists of the cyber security service established minutes after [the incident] that the enterprise's process control system and system for detecting signs of emergencies had deliberately been infected by the VPN Filter computer virus originating from Russia," the SBU said. Workers at the chlorine company worked with its telco providers and cyber security experts at the SBU to thwart the purported attack, the agency said.

Workers at the chlorine company worked with its telco providers and cyber security experts at the SBU to thwart the purported attack

Fitness App exposed Data of Military Personnel and Spies

Source: https://threatpost.com/

Fitness device maker Polar Flow suspended an Explore tracking feature on its mobile app after researchers discovered profile

"With only a few clicks, a high-ranking officer of an airbase known to host nuclear weapons can be found jogging across the compound in the morning."

and geo-location data of high-ranking military personnel and spies that were being exposed to the public on its network. "With only a few clicks, a high-ranking officer of an airbase known to host nuclear weapons can be found jogging across the compound in the morning. From a house not too far from that base, he started and finished many more runs on early Sunday mornings. His favourite path is through a forest, but sometimes he starts and ends at a car park further away. The profile shows his full name," wrote Foeke Postma, a researcher with investigative site Bellingcat. Polar stressed no private data was "leaked" and in a precautionary move it turned off the Explore function of its app as on July 6.

Cybercriminals are preparing Global Fraud 'ATM Cash-out'

Source: https://krebsonsecurity.com/

"Historic compromises have included small-to-medium size financial institutions, likely due to less robust implementation of cyber security controls, budgets, or third-party vendor vulnerabilities,"

The Federal Bureau of Investigation (FBI) warned banks that cybercriminals are preparing to carry out a highly choreographed, global fraud scheme known as an 'ATM cash-out' in which they hack a bank or payment card processor and use cloned cards at cash machines around the world to fraudulently withdraw millions of dollars in just a few hours. Just prior to executing on ATM cash-outs, the intruders remove many fraud controls at the financial institution, such as maximum ATM withdrawal amounts and any limits on the number of customer daily ATM transactions. The perpetrators also alter account balances and security measures to make an unlimited amount of money available at the time of the transactions, allowing for large amounts of cash to be quickly removed from the ATM. Virtually all ATM cash-out operations are launched on weekends, often just after financial institutions begin closing for business on Saturday. "Historic compromises have included small-to-medium size financial institutions, likely due to less robust implementation of cyber security controls, budgets, or third-party vendor vulnerabilities," the alert says. FBI alert is related to a breach of the Cosmos Cooperative Bank in India, where thieves used cloned cards to execute 12,000 transactions and stole roughly $13.5 million via 25 ATMs located in Canada, Hong Kong and India.

Hackers in Detroit Steal over 600 Gallons of Gasoline

Source: https://gizmodo.com/

Hackers in Detroit managed to hack a gas pump and steal over 600 gallons of gasoline, valued at about $1,800. The theft took place in the middle of the day and went on for about 90 minutes, with the gas station attendant unable to thwart the hackers.

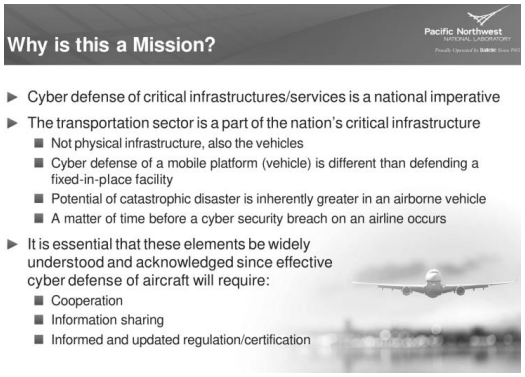
It is supposed that the thieves used some sort of remote device that allowed them to hijack the pump and take control away from the gas station employee. Also the device prevented the clerk from using the gas station's system to shut off the individual pump. It appears that the attackers would have targeted the fuel-management software used by the gas station. These systems have long been considered potential targets because many include web-based interfaces.

It appears that the attackers would have targeted the fuel-management software used by the gas station.

DHS Team successfully Remotely Hacked a Boeing 737

Source: https://motherboard.vice.com

US government researchers believe it is only a matter of time before a cybersecurity breach on an airline occurs, according to documents obtained by Motherboard. The comment was included in a recent presentation talking about efforts to uncover vulnerabilities in widely used commercial aircraft, building on research in which a Department of Homeland Security (DHS) team successfully remotely hacked a Boeing 737. In 2016, the DHS S&T established a multi-agency group to carry out cybersecurity vulnerability evaluations of airplanes. That same year, the team of government, industry, and academic officials demonstrated how to remotely hack a commercial aircraft in a non-laboratory setting, trade publication Avionics reported. "Today's commercial aviation backbone is built upon a network of trust; most commercial aircraft currently in use have little to no cyber protections in place," a DHS presentation says.



A section of a PNNL presentation obtained by Motherboard

"Today's commercial aviation backbone is built upon a network of trust; most commercial aircraft currently in use have little to no cyber protections in place,"

Trends

Rising Cyber Crime Trends

Sh. Abhijeet Raj Shrivastava, Sectoral Coordinator, Transport, NCIIPC

Cybercrime trends that are rising in recent years and will further impact organisations are listed below.

'Fileless' Attacks: Cyber-criminals are using 'Fileless' attacks leveraging trusted Windows executable to invade systems and compromise organisation networks. 'Fileless' attacks does not drop malware on a compromise system, it uses tools already installed on computers or run simple scripts and shellcode in memory, often hidden in the Windows Registry. CactusTorch is one such 'Fileless' attack that uses the 'DotNetToJScript' technique which loads and executes malicious .NET assemblies straight from memory. [1]

'Fileless' attacks does not drop malware on a compromise system, it uses tools already installed on computers.

Crypto-currency Hijacking: Cybercrime is trending towards crypto-currency hijacking, which coincided with the increased market interest in digital currencies.

Cybercriminals are looking for computing power of compromise machines that forms the part of bot's instead of using their own equipment because the price of a dedicated mining machine could exceed $5,000. [2]

Urban critical infrastructure such as electric grids, water networks and transportation systems are prime targets for cyber-attacks.

SIM Swap Fraud: SIM swap fraud is a type of identity theft and rely on phone-based authentication has made SIM swapping an increasingly lucrative business. It allows hackers to gain access to bank accounts, credit card numbers, and other personal data. It's tough to spot, and even tougher to undo the resulting damage. Social engineering is mostly used for gaining personal information of user's SIM. [3]

SCADA Systems Cyber-attacks: Traditional SCADA systems lack proper security measures. However, with the integration of complex new architectures with future Internet based solutions on the concepts of IoT, cloud computing, mobile wireless sensor networks, and so on, there are many issues at stakes in the security and deployment of these classical systems.

Urban critical infrastructure such as electric grids, water networks and transportation systems are prime targets for cyber-attacks. These systems are composed of connected devices which we call the Industrial Internet of Things (IIoT). [4]

Recently, the AI.type keyboard app that learns users' writing styles to create a personalized messaging experience suffered a leak that exposed 31 million Android users. Hackers were able to gain access to their server containing user's names, emails and exact location, along with how long the app had been installed on their device.

Mobile Malwares: Mobile Malwares campaigns targeting users on the Google Play stores from very beginning. From the very first banking Trojan on Google Play, dubbed Droid09, to the latest ad-click fraud/Bitcoin-mining latent apps that plague the store week after week today. [5]

Artificial Intelligence Based Cyber-attacks: India witnessed AI-powered cyber-attack, where machine learning was used to study patterns of normal user behaviour within a company's network. Recently, the AI. type keyboard app that learns users' writing styles to create a personalized messaging experience suffered a leak that exposed 31 million Android users. Hackers were able to gain access to their server containing user's names, emails and exact location, along with how long the app had been installed on their device. Automated bot attacks will continue to make a splash. [6]

References:

[1] https://www.hindustantimes.com/tech/fileless-cyber-attacks-on-the-rise-in-2018-mcafee-report/story-zaXiguE1Hkm9tL2wd0rKLP.html

[2] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2018.pdf

[3] https://www.digitaltrends.com/mobile/sim-swap-fraud-explained/

[4] http://creativecommons.org/licenses/by/3.0/

[5] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf

[6] https://www.csoonline.com/article/3246196/cyberwarfare/2018-the-year-of-the-ai-powered-cyberattack.html

China using Artificial Intelligence to Track 1.4 Billion People

Source: https://www.nytimes.com

With millions of cameras and billions of lines of code, China is making use of technologies like facial recognition and artificial intelligence to identify and track 1.4 billion people. Cameras scan train stations for China's most wanted. Billboard-size displays show the faces of jaywalkers and list the names of people who don't pay their debts. Facial recognition scanners guard the entrances to housing complexes. Already, China has an estimated 200 million surveillance cameras — four times as many as the United States. "The whole point is that people don't know if they're being monitored, and that uncertainty makes people more obedient," said Mr. Chorzempa, the Peterson Institute fellow.

A video showing facial recognition software in use at the headquarters of the artificial intelligence company Megvii in Beijing

US Army conducting Cyber Exercises in Physical Training Space

Source: https://federalnewsradio.com

US Army with help from the SANS Institute, is beginning to conduct its cyber exercises in a physical training space that closely resembles a fully-functioning city. 400-acre Muscatatuck Urban Training Complex, in south-eastern Indiana has a port, a functioning power grid, complete with all of the programmable logic controllers one might find in a real-world system, a subway station, a water treatment plant, and many other features of modern urban life a foreign power might target in an actual cyber-attack. "We run a lot of these scenarios where it's just the fingers on keyboard piece, and you learn a lot from that. But until you go up to full-scale, you can't really appreciate how all of this stuff really comes together," said Ed Skoudis, SANS' director for cyber ranges.

400-acre Muscatatuck Urban Training Complex has a port, a functioning power grid, a subway station, a water treatment plant, and many other features of modern urban life a foreign power might target.

Regular Expression Denial of Service Attack

http://mp.binaervarianz.de/ReDoS_TR_Dec2017.pdf

Compared to a regular DoS attack, ReDoS vulnerability enables an attacker to launch an attack with fewer resources.

Regular Expression Denial of Service (ReDoS) is a class of algorithmic complexity attacks where matching a regular expression against an attacker-provided input takes unexpectedly long. Compared to a regular DoS attack, ReDoS vulnerability enables an attacker to launch an attack with fewer resources. For example, matching the regular expression /(a+)+b/ against a sequence of 30 'a' characters on the Node.js JavaScript platform takes about 15 seconds on a standard compute. Matching a sequence of 35 'a' characters take over 8 minutes, i.e., the matching time explodes exponentially. An attacker can exploit it to overwhelm the server with hard-to-match inputs. Defences to overcome this vulnerability:

- To limit the effect of a payload delivered through an HTTP header, the size of the header should be limited.
- To use a more sophisticated regular expression engine that guarantees linear matching time.
- To add a timeout parameter which will stop any matching of regular expressions that takes longer than the specified timeout.

https://apps.nga.mil/Home/Store

US creates an App Store for all Defence Groups

Source: https://www.wired.com

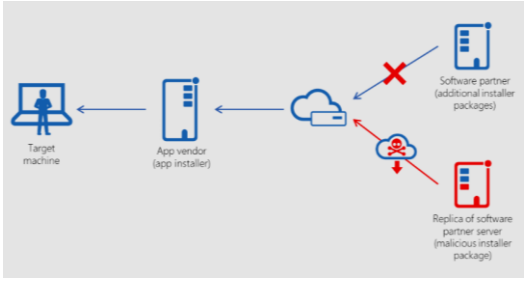
NGA's GEOINT App Store runs its security protections and screening processes in a way a commercial platform can't by getting developers to agree to hand over the source code of their apps for in-depth analysis and review to avoid any malware in the apps.

US National Geospatial-Intelligence Agency (NGA) has created an app store for all defence groups to provide sensitive and mission-critical apps. NGA's GEOINT App Store runs its security protections and screening processes in a way a commercial platform can't by getting developers to agree to hand over the source code of their apps for in-depth analysis and review to avoid any malware in the apps. The agency contracted with a private firm called Engility to directly manage the outreach, acquisition, and development environment of App store. The inspection is always mediated by Engility, which signs nondisclosure agreements with developers and isn't a software maker itself. The brokered vetting process means that the government never holds developers' source code directly which made developers to share their source code with a non-disclosure agreement which eventually leads to in-depth analysis of app and only Safe and clean apps go into their app store which makes this app store safe and secure compared to commercial app-stores.

Malware Bytes

Microsoft discovers a Supply Chain Attack on PDF Editor App

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

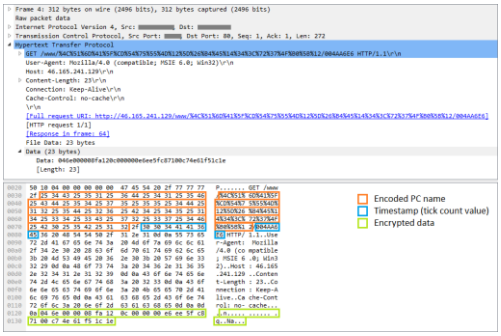


Microsoft discovered a supply chain attack where hackers compromised a font package installed by a PDF editor app and used it to deploy a cryptocurrency miner on users' computers. Hackers breached the cloud server infrastructure of a software company providing font packages as MSI files. Attackers recreated the cloud infrastructure on a replica server and hosted all MSI files, including font packages, all clean and digitally signed, in the replica server. Attackers decompiled and modified one MSI file, an Asian font's pack, to add the malicious payload with the coin mining code. These MSI files were offered to other software companies. One of these downstream companies was using these font packages for its PDF editor app, which would download the MSI files from the original company's cloud servers. The attackers were able to influence the download parameters used by the PDF editor app that pointed to the attacker server. Because the PDF editor app was installed under SYSTEM privileges, the malicious coinminer code hidden inside would receive full access to a user's system. The malicious miner would create its own process named xbox-service.exe under which it would mine for cryptocurrencies using victims' computers.

Attackers decompiled and modified one MSI file, an Asian font's pack, to add the malicious payload with the coin mining code. These MSI files were offered to other software companies.

ESET discovers Highly Targeted Malware active since 2013

Source: https://www.welivesecurity.com



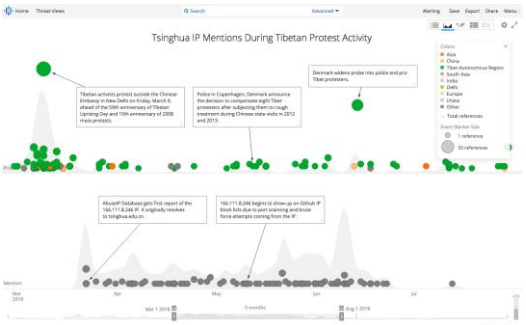
A request sent to the C&C server

ESET has discovered a highly targeted InvisiMole malware that have been active at least since 2013, yet was never detected. Only a few dozen high-profile computers have been found to be infected. InvisiMole has a modular architecture, starting its journey with a wrapper DLL which is placed in the Windows folder, masquerading as a legitimate mpr.dll library file. It performs its activities using two other modules which contain various commands to make system changes and spying. Malware protects itself from the eyes of administrators by encrypting its data and communication. It is able to reach out to the C&C servers even if there is a proxy configured on the infected computer. C&C communication consists of a series of HTTP requests. The encrypted request includes a PC identifier, timestamp and other data. It is capable of remotely activating the microphone on the compromised computer, capturing sounds and taking screenshots. The malware also monitors all fixed and removable drives mapped on the local system. Whenever a new drive is inserted, it creates a list of all the files on the drive and stores it encrypted in a file.

Only a few dozen high-profile computers have been found to be infected.

To prevent the recovery of deleted files, the malware has ability to safe-delete all the files, which means it first overwrites the data in a file with zeroes or random bytes, and only then is the file deleted.

InvisiMole is capable of recording SSID and MAC address of the visible Wi-Fi access points on compromised machine which can be used to obtain geolocation of the victim. Malware always restores the original file access or modification times, so that user is unaware of its operation. The collected data is temporarily stored in files and deleted once it is sent to the C&C servers. To prevent the recovery of deleted files, the malware has ability to safe-delete all the files, which means it first overwrites the data in a file with zeroes or random bytes, and only then is the file deleted.



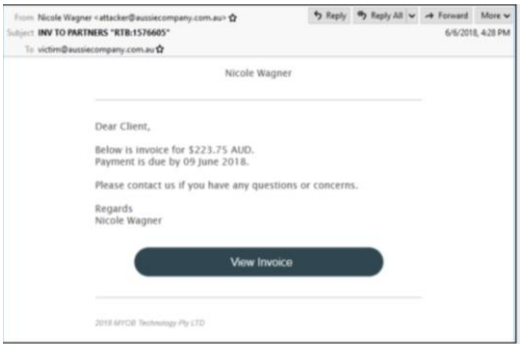
Recorded Future timeline of Tsinghua IP activity in correlation with Tibetan protests

In several cases, these activities occurred during periods of Chinese dialogue for economic cooperation with these countries or organizations.

Reconnaissance Activities Supporting China's Economic Goals

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

Recorded Future's Insikt Group identified a Linux backdoor called 'ext4' deployed against the Tibetan group. By analysing the backdoor, repeated attempted connections to some compromised CentOS web server emanating from infrastructure registered to Tsinghua University was uncovered. Network reconnaissance activities being conducted from the same Tsinghua University infrastructure targeting many geopolitical organizations, including the State of Alaska Government, Alaska's Department of Natural Resources, the United Nations office in Nairobi, and the Kenya Ports Authority were also found. The targeted scanning of German automotive Daimler AG was identified a day after it cut its profit outlook for the year, citing the growing trade tensions between the U.S. and China. In several cases, these activities occurred during periods of Chinese dialogue for economic cooperation with these countries or organizations. Recorded Future assesses with medium confidence that the network reconnaissance activities were conducted by Chinese state-sponsored actors in support of China's economic development goals.



Fake MYOB invoice phishing email sent by attackers

DanaBot Banking Trojan Phishing Campaign with Fake Invoices

Source: https://threatpost.com/

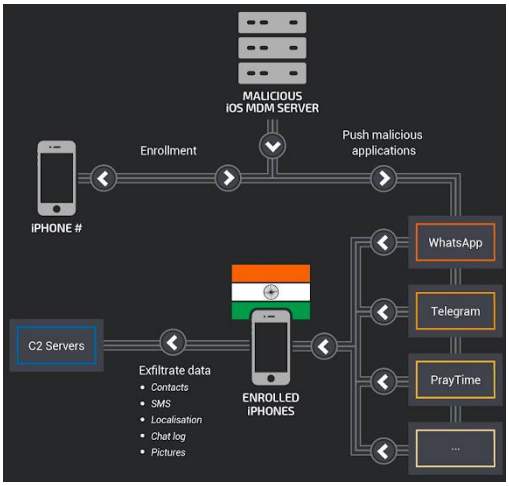
DanaBot is a banking Trojan discovered in May targeting users in Australia via emails containing malicious URLs. The recently-discovered phishing campaign targets potential victims with fake invoices from Australian software company MYOB. Attackers send fake invoice messages with links pointing to compromised FTP servers hosting the DanaBot malware. In clicking 'View Invoice' button a zip archive is pulled down from a compromised FTP server of an Australian company. Contained inside the .Zip archive is a JavaScript downloader that when executed downloads the DanaBot Trojan.

Once downloaded it steals private and sensitive information, and sends screenshots of the machine's system and desktop to the Command and Control server.

Highly Targeted Campaign against Indian iPhones

Source: https://blog.talosintelligence.com

Cisco Talos has identified a highly targeted campaign against 13 Indian iPhones. It is unclear who the targets of the campaign were, who was the perpetrator, or what the exact purpose was. It's very likely the vector for this campaign was simply social engineering - in other words asking the user to click 'Ok'. The attackers installed an open-source Mobile Device Management (MDM) and used this to deploy malicious code into secure chat applications such as Telegram and WhatsApp to steal the messages, photos and user's location from the victim's phone. Over a three-year period, the attackers remained under the radar — likely due to the low number of compromised devices. All the technical details point to an actor based in India. The attacker tried to mimic Russian hackers by using mail.ru email. However, testing devices enrolled on MDM was of an Indian phone number registered on an Indian provider.



Learning

Vulnerability Analysis of Smart Meters

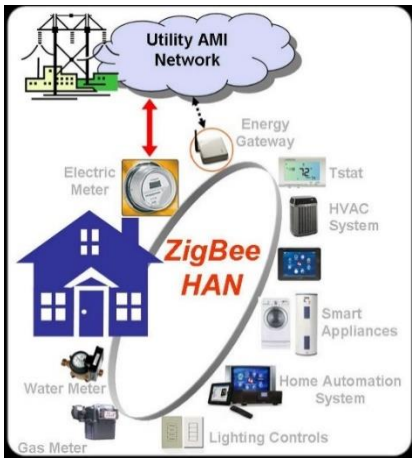
Sh. Arun Sharma, NCIIPC

The Power & Energy Sector is edging towards Smart Grid, also known as Advanced Metering Infrastructure – AMI, which has the ability to remotely monitor and control all grid activities. However, the networked controllable electricity meters, play an important role in assuring the security of the Smart Grid. Smart Meters would be installed in each home, and can be easily interfere by many people. As the physical protection would be limited, it is simple to assume that keen customers would inspect the devices to try and understand its internal working. It is new technology product and there may be scope to improve standardization with respect to security. As many different vendors would develop their own software Applications, with a possibility that Smart Meter software would be vulnerable to attacks. Some of the possible attack vectors are as following:

Reflecting a metering unit

The networked controllable electricity meters, play an important role in assuring the security of the Smart Grid

Exposure of Secret Data: Vulnerabilities in Smart Meters that leads to knowledge of electricity usage information can be



An AMI Network paradigm

used to predict the point of presence of someone in the premises.

Meter Tampering: Attackers can do modification in the bill of victim's units.

Pivoting: Since, Smart Meters would be connected through GSM Network; it would be easy to enter and penetrate into the smart device of home and access the free calls / Internet connectivity. Also, it could lead to vital information about Smart Grid Network.

Remote Command Execution: Remote access to Smart Meters can lead to remotely switch off its internal safety & security mechanics. Hence, this may lead to damage of Smart Meter.

Grid Destabilization: With remote accessibility of Smart Meters, an attacker could gain control of hundreds or thousands of identical metering devices, and exploit vulnerabilities to simultaneously switch heavy loads with the intention of to destabilize and bring down the power grid on heels. [1]

With remote accessibility of Smart Meters, an attacker could gain control of hundreds or thousands of identical metering devices, and exploit vulnerabilities to simultaneously switch heavy loads with the intention of to destabilize and bring down the power grid

A black-box approach called Fuzzing is universally used to find vulnerabilities in proprietary embedded software of Smart Meters. It provides an intelligent approach towards injecting irregular message content and data inputs in order to qualify the robustness of a system. There are well acknowledged frame works present to fuzz the complex scenarios in Smart Metering as following:

SPIKE: SPIKE is designed to assist in the creation of network oriented fuzzers and supports sending data via TCP or UDP.

SNOOZE: An acronym for 'Stateful NetwOrk prOtocol fuzZEer', identifies security flaws in network protocol implementation.

Peach: Peach is a smart fuzzer, capable of performing both generation & mutation-based fuzzing. [2]

On a world-wide canvas, Government Communications Headquarters (GCHQ) has warned that UK's Smart Meters could be vulnerable to Cyber Attacks. [3] Korea is marching towards the Smart Grid Advanced Metering Infrastructure (AMI), and has selected the Device Language Message Specification / COmpanion Specification for Energy Metering (DLMS/COSEM) protocol for the Smart Meter Communications. Smart Grid AMI is being tested and operated in Korea. [4]

Ways for identifying potential attack vectors and associated risks and vulnerabilities in Smart Meters, can be listed out as under:

- Static Source Code Analysis
- Penetration Testing
- Dynamic Analysis and Fuzzing
- Exploratory Testing and Manual Code Auditing
- Backdoor Detection

Security issues need immediate attention prior to large-scale roll-outs of Smart Meters in India

Thus, security issues need immediate attention prior to large-scale roll-outs of Smart Meters in India. [1]

References:

[1] Deft University of Technology: http://repository.tudelft.nl/

[2] Gray Hat Hacking – Tata McGraw Hill Publication

[3] https://www.information-age.com/smart-metres-vulnerable-cyber-attacks-123470837

[4] https://ieeexplore.ieee.org/document/7917173/

Compromised System Identification in a Network

Sh. Ankit Sarkar and Sh. Shiv Charan Kataria, NCIIPC

A compromised system in a network can spell doom the security of an entire information infrastructure. A compromise could be a result of any kind of cyber-attack. Some cyber criminals want data, some want a ransom, and some simply want a disruption in continuity. Cyber Criminals targets any end-point device that may be a server or an end-user device. Common ways to execute a cyber-attack are:

- Viruses
- Worms
- Adware/Spyware
- Trojans
- Social Engineering
- Man in the Middle
- Drive-by
- Ransomware

A compromised system in a network can spell doom the security of an entire information infrastructure.

Repeated attempts to connect to any outside machine without any request from that IP indicates a possible infection and the infected system is trying to connect to its command & control server.

Most organizations prioritise securing data rather than devices. Identifying systems/devices becomes extremely important to ensure integrity, confidentiality and business continuity. A regular analysis comprising the following factors while monitoring network traffic can help identify compromised systems:

Connections to IPs: When there are connections to or attempts to connect to (Full form) IPs that are blacklisted or with low rating/reputation. Repeated attempts to connect to any outside machine without any request from that IP indicates a possible infection and the infected system is trying to connect to its command & control server. The target IP may not be the actual (Full form) C&C but another infected machine. Another way to spot potential threat traffic is to look at anomalous destination domains or IP addresses. Those that are new, as well as lower-volume, can indicate suspicious outbound traffic.

Unwarranted Internal Connections: Internal network devices creating unwarranted connection when there should be none or at least known indicates a compromised machine trying to spread its infection or recce to identify more targets in the network.

Unrecognised Protocols: Port used in network communications generally identifies with a respective application responsible for the traffic. Many instances of malware communicate by using a proprietary application or service, the traffic can be sent over a completely unknown port indicating opening of unwanted ports. This analysis is quite simple, requiring observation only of traffic that originates from endpoints outside the normally allowed ports. A compromised machine at least attempts to communicate in its programmed manner. So looking for communication attempts from endpoints can help to identify compromised systems, even when those attempts are unsuccessful.

Traffic Patterns: Malware depends on few specific uses of outbound communication. It often connects to (Full form) C&C to obtain next set of commands. Key-loggers may have patterns of connections in small bits. There may be either unknown connection attempts or unusual amounts of traffic through the allowed ports. A routine spike in traffic calls for an analysis. In some cases, the allowed ports are used when the intended application using that port is not active.

Masquerading Protocols: One of the ways a malware tries evading detection is by hijacking a known protocol's port. Identification of this requires looking beyond the assumed purpose of the port and then analysing and matching with the genuine traffic generated through the port and application

DNS Queries: Modification of DNS settings to point to an attacker's server has been an effective technique. This enables the attacker to cause further redirection. DNS should have few source IPs as the protocol should be centralised with a few internal DNS servers.

Known Signatures: Most malware leave a trail of consistent traffic patterns which can help in generating a database of known signatures. Comparison of traffic with the signature database can then be done using Deep Packet Inspection Techniques. However, using this method effectively requires efforts to be updated with the signature databases.

Disabled/Banned Protocols: A number of protocols are used but are banned for general use within internal systems. Protocols such as SMTP, SSH, VPN, RPC and IRC are either used in IT sanctioned cases or are completely banned. Analysing the use of these prohibited protocols can thus help indicating threat traffic.

Protocols such as SMTP, SSH, VPN, RPC and IRC are either used in IT sanctioned cases or are completely banned. Analysing the use of these prohibited protocols can thus help indicating threat traffic.

DLP Indicators: Data Loss Prevention (DLP) solutions classify data patterns and review traffic for any instance of that pattern. These then block copy of files, drop attachments and so on when the pattern is identified

In short, by monitoring the network traffic, a lot can be determined about the status of the health of the machines in the network. Regular monitoring enables the insight into abnormal behaviour and helps identify such behaviour by pin pointing variations.

References:

[1] www.logrythm.com

[2] www.itgovernance.co.uk

IoT Security for Power & Energy Sector Companies

Sh. Ganesh Kumar Sahu, Sectoral Coordinator, NCIIPC

Power & Energy Sector is one of the most critical due to the interdependencies of other critical sectors. Organisations under this sector need to take proactive measures for protecting their Information Infrastructure. These organisations must also operate their critical business processes more effectively and efficiently to meet consumer and government expectations. To achieve these objectives, companies are going for new technologies, including the Internet of Things (IoT) and Industrial IoT (IIOT). IoT devices cover a very broad spectrum of purpose, and companies are deploying these interconnected devices in their operations at a rapid pace. They use them to collect operational data, monitor operational technology performance, control processes at the edge, and capture consumer usage and performance.

For this reason, the growth of the IoT technology within the power and energy sectors is going to increase in near future. But along with this rapid increase in IoT devices comes a proportional increase in cybersecurity risk. Organizations need to protect themselves against the cybersecurity risks posed by deploying IoT technologies in their operations and factories. It also needs to determine the capabilities needed to identify, protect, respond to and recover from IoT cyber incidents. Industry and utilities companies, in particular, need to develop new strategies to mitigate and manage cyber-risks. IoT devices are huge in number spread all across utility operations in terms of smart meters, sensors, alarms etc. It makes sense that these industries use IoT for things such as real-time data analytics, equipment monitoring, predictive maintenance and machine automation. The outbreak of such IoT technology facilitates the utility companies but at same time brings about number of cybersecurity challenges as this technology increases cyber threat surface area due to presence of vulnerabilities in IoT devices and sensors. To mitigate IoT security risk and improve performance, utility companies can implement best practices:

Encryption to protect against attacks that could gain access to sensitive information such as user credentials and lead to the disruption of service and destruction of Intellectual property and equipment, or create personal safety issues

- Increase employee visibility into IoT security operations, IT and OT. Manufacturers of next-generation connected devices and services may consider purchasing insurance against software malfunctions and any damage hackers might cause.
- Technical details of each endpoint IoT device such as it communicates to which access point and which protocol is used for communication. Every IoT endpoint must be identified and profiled, added to an asset inventory and monitored.
- Define clear SLAs where there is reliance on partners and system integrators. Form a cross-functional security team made up of IT security, engineering, operations and a control system vendor.
- To prepare an effective response to cyberattacks, carry out Cyber security drills for situational awareness along with Security Operation Centre (SOC) monitoring.

In order to protect their Critical Information Infrastructure, utility companies can deploy technologies such as:

- Proper access control mechanism between access point and IoT devices with end to end encryption or VPN.
- SOC monitoring to identify potential IoT attacks and intrusions that may have by passed existing security controls.
- Encryption to protect against attacks that could gain access to sensitive information such as user credentials and lead to the disruption of service and destruction of Intellectual property and equipment, or create personal safety issues.

- Network security and device authentication, to secure deployments between IoT devices, gateways, servers and applications.

References:

[1] https://www.infineon.com/cms/en/applications/smart-card-and-security/iot-security/

[2] https://securityintelligence.com/at-your-own-risk-managing-internet-of-things-iot-risks-for-industrial-and-utility-companies/

MPLS Network and its Challenges

Sh. Ashok Kumar Gupta, NCIIPC

Multi-Protocol Label Switching (MPLS) is a type of data-carrying technique for high-performance telecommunications networks which provides a mechanism for forwarding packets for any network protocol. It was originally developed in the late 1990s to provide faster packet forwarding for IP routers. Since then its capabilities have expanded massively, for example to support service creation Virtual Private Network, Traffic Engineering, Network Convergence, and increased resiliency. MPLS is now the de-facto standard for many carrier and service provider networks and its deployment scenarios continue to grow.

MPLS similarly uses IP addresses, either IPv4 or IPv6, to identify end points and intermediate switches and routers. This makes MPLS networks IP-compatible and easily integrated with traditional IP networks. However, unlike traditional IP, MPLS flows are connection-oriented and packets are routed along pre-configured Label Switched Paths (LSPs).

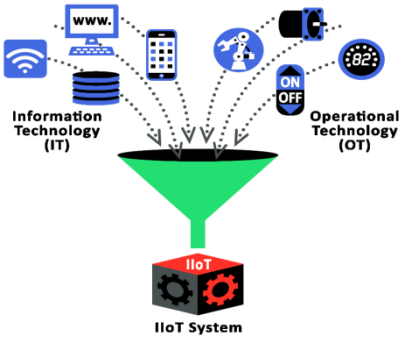
It was originally developed in the late 1990s to provide faster packet forwarding for IP routers. Since then its capabilities have expanded massively, for example to support service creation Virtual Private Network (VPNs), Traffic Engineering, Network Convergence, and increased resiliency.

The evident power of the basic MPLS concepts led the industry to define generalized extensions to MPLS, or Generalized MPLS (GMPLS). This work extended the MPLS concept of a label to include implicit values defined by the medium that is being provisioned, for example a wavelength for a DWDM system or a timeslot for a SONET/SDH device. So, with GMPLS, there is no need for a switch to 'read' the label in each packet header. The label is an inherent part of the switch fabric and the switching operations depend on wavelength, or timeslot etc. This permits the benefits of MPLS to be shared by many different types of switching platform.

MPLS process can be considered as Critical Information Infrastructures (CII) in Telecom Sector. One of the biggest challenges is deploying the right strategies and expertise to build, maintain and run an MPLS network. There is always a need for quick proactive and reactive approach whenever there is a problem in the MPLS network.

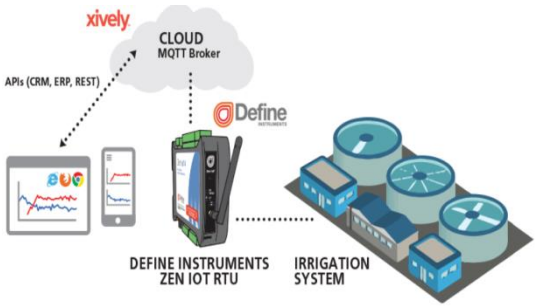
IIoT Risk and Countermeasures

Sh. Niraj Vishnoi, NCIIPC



Over the past few decades, increasingly affordable computing power, ubiquitous connectivity and evolving data analytics techniques have opened the door to convergence of control systems, business systems and the Internet. In the past, there has been a strong separation between IT and OT. IT covers computer and communication systems common across industries. Software applications are people-centric, and risks are often low. OT, on the other hand, is a combination of hardware (initially) and software (more recently) that collects information and causes changes in the physical world through the direct monitoring and control systems. Control of physical systems are task-specific, customized, automated and require less user interaction.

An Industrial Internet of Things (IIoT) system connects and integrates industrial control systems with enterprise systems, business processes and analytics. An IIoT system enables significant advances in optimizing decision-making, operations and collaborations among a large number of increasingly autonomous control systems [1].



Remote Monitoring and Control of a large water filtering station for irrigation is an example of IIoT. Xively platform is used for Cloud Platform Provider. A typical IIoT system uses a broker (an intermediary program module that translates a message from the formal messaging protocol of the sender to the formal messaging protocol of the receiver) in the Cloud. In this system MQTT (Message Queuing Telemetry Transport) broker is used as it is available in most Cloud systems. Coupled with this is the Define Instruments Zen IoT RTU. The difference between this and the traditional RTU is that it is setup to deliver messages to the Cloud broker using MQTT. It uses publish and subscribe model. The Zen IoT RTU will publish information like pressure and flow rate to the broker and subscribe to a control topic [2].

Risk of IIoT System: IIoT interact with the physical world where uncontrolled change can lead to hazardous conditions. This potential risk increases the importance of safety, reliability, privacy and resiliency beyond the levels expected in many traditional IT environments.

A successful attack on an IIoT system has the potential to be as serious as the worst industrial accidents to date (e.g. Chernobyl), resulting in damage to the environment, injury or loss of human life.

A successful attack on an IIoT system has the potential to be as serious as the worst industrial accidents to date (e.g. Chernobyl), resulting in damage to the environment, injury or loss of human life. There is also risk of secondary damage such as disclosure of sensitive data, interruption of operations and destruction of systems during such an attack. The results of attacks on IIoT systems may be widespread and comparable to large natural disasters, but stemming from malicious intent.

This will result in damage to brand and reputation, material economic loss and potential damage to critical infrastructure [1].

According to the Global ICS and IIoT Risk Report [4], published in October 2017, by OT security firm CyberX, one-third of the OT networks whose processes are controlled by Industrial Control Systems (ICS) are exposed to the public Internet. Half lack anti-virus protection and more than half use easily hackable plain-text passwords in their control networks. More than three-quarters run obsolete Windows systems like XP and 2000 that are unsupported with security patches, while 82 percent run well-known remote access management protocols, making it easier to access and manipulate network equipment. 22 percent have wireless access points, which can be compromised in multiple ways, including the KRACK WPA2 vulnerability in most Wi-Fi networks [3].

One-third of the OT networks whose processes are controlled by Industrial Control Systems (ICS) are exposed to the public Internet

Countermeasures:

Implement a multi-layered defence with continuous monitoring: SANS refers to this multi-layered approach as "Active Cyber Defence." As defined by SANS, it's the process of using security operations to continuously identify and counter threats. The Active Defence Cycle consists of four phases that continuously feed each other to create an ongoing process: asset identification and network security monitoring; incident response; threat and environment manipulation (e.g., addressing vulnerabilities); and threat intelligence consumption.

Proactively address the most critical vulnerabilities: It's seldom practical to remediate or mitigate all vulnerabilities, start by identifying most critical assets — such as devices controlling most important production processes — and then perform automated threat modelling to identify and address the most likely attack paths to those assets.

Educate plant workers and enforce strong corporate policies: In corporate IT networks, raising awareness of risky behaviours can go a long way to reducing risk.

Break down the barriers between OT and IT: IT and OT teams have a lot to teach each other about their respective disciplines. Management needs to create a top-down culture that fosters a belief that "we're all in this together, so let's help each other." One way to start is by integrating OT personnel into your Security Operations Centre (SOC). Another is to assign IT security people to the OT organization for temporary assignments, so they learn first- hand how control systems work. [4]

One way to start is by integrating OT personnel into your Security Operations Centre (SOC). Another is to assign IT security people to the OT organization for temporary assignments, so they learn first- hand how control systems work.

References:

[1] https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

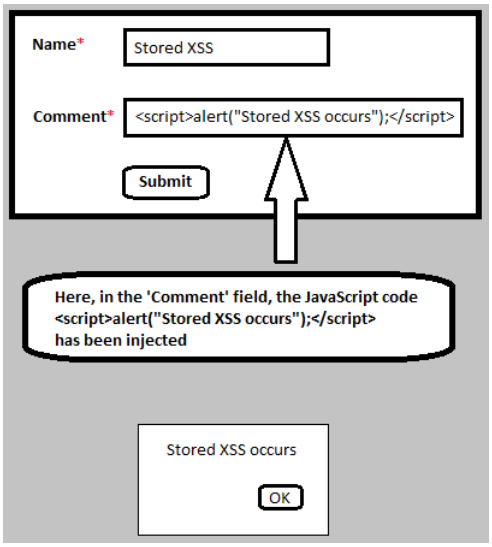
[2] http://www.defineinstruments.com/blog/scada-systems-vs-iiot-solutions

[3] https://www.eetimes.com/document.asp?doc_id=1333145

[4] https://cyberx-labs.com/en/risk-report-2017

Stored XSS is the most Dangerous Type of XSS

Source: https://securitycommunity.tcs.com/



Injecting any kind of malicious payload in feedback field for an article permanently is an example of Stored XSS.

Cross-site Scripting (XSS) vulnerability refers to code injection attack in client-side where malicious scripts or payloads can be executed by an attacker into a trusted website. Stored XSS poses high risk because inputs injected by the attacker is stored and embedded into the vulnerable web application permanently in an unsafe way. It does not need any isolated delivery mechanism for reaching out to the target users. The end users do not require clicking on a malicious link in order to run or execute the script; simply just he/she needs to visit the affected page of the web application once in a browser. Injecting any kind of malicious payload in feedback field for an article permanently is an example of Stored XSS. Impact of XSS vulnerability varies from application to application. A victim may face a variety of problems ranging in severity from an annoyance to the full compromise of the application. In order to prevent Stored XSS attacks, the best way is to handle the input securely in both client-side and server-side in a proper manner before it gets stored permanently on the web server. When secure input handling does not work, at that time Content Security Policy comes into play to provide an additional layer of defence. Modern web browsers have an inbuilt XSS filter. Additionally X-XSS-Protection: 1; mode=block header can be added to particular site.

Vulnerability Watch

Critical Vulnerability in VMware AirWatch Agent

https://nvd.nist.gov/vuln/detail/CVE-2018-6968

This vulnerability may allow for unauthorized creation and execution of files in the Agent sandbox

A critical vulnerability (CVE-2018-6968) has been found in VMware AirWatch Agent. It has a CVSSv3 Base Score of 10. The VMware AirWatch Agent for Android prior to 8.2 and AirWatch Agent for Windows Mobile prior to 6.5.2 contain remote code execution vulnerability in real time File Manager capabilities. This vulnerability may allow for unauthorized creation and execution of files in the Agent sandbox and other publicly accessible directories such as those on the SD card by a malicious administrator. VMware has issued a fix for it.

Critical Vulnerability in Apple MacOS Products before 10.13.5

https://nvd.nist.gov/vuln/detail/CVE-2018-4229

Critical security features vulnerability (CVE-2018-4229) was found in the Apple macOS products before 10.13.5. The affected component is 'Grand Central Dispatch'. It has a CVSSv3 Base Score of 10. In this issue a sandboxed process may be able to circumvent sandbox restrictions. It allows attackers to bypass a sandbox protection mechanism by leveraging the mis-parsing of entitlement plists. This issue was addressed with improved input validation. Users are advised to use security update to fix this issue.

It allows attackers to bypass a sandbox protection mechanism by leveraging the mis-parsing of entitlement plists.

Critical Vulnerability in Safe-eval Module

https://nvd.nist.gov/vuln/detail/CVE-2017-16088

Improper Access Control vulnerability (CVE-2017-16088) has been found in safe-eval module. It has a CVSSv3 Base Score of 10. Affected versions of safe-eval are vulnerable to a sandbox escape. By accessing object constructors, un-sanitized user input can access the entire standard library and effectively break out of the sandbox. The safe-eval module describes itself as a safer version of JavaScript eval().

The safe-eval module describes itself as a safer version of JavaScript eval().

Critical Vulnerability in Oracle Database Server

https://nvd.nist.gov/vuln/detail/CVE-2018-3110

A critical vulnerability (CVE-2018-3110) was discovered in the Java VM component of Oracle Database Server. It has a CVSSv3 Base Score of 9.9. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18. The vulnerability can be exploited over 'Oracle Net' protocol. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. While the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java VM. Users are advised to upgrade to latest version.

Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM.

Multiple Critical Vulnerabilities in Quick Emulator

Source: https://nvd.nist.gov

Quick Emulator (QEMU), built with the Cirrus CLGD 54xx VGA Emulator and the VNC display driver support, is vulnerable (CVE-2016-9603) to a heap buffer overflow issue. The issue could occur when a VNC client attempts to update its display after a VGA operation is performed by a guest.

A privileged user/process inside guest could use this flaw to crash the QEMU process resulting in DoS or, potentially, leverage it to execute arbitrary code on the host with privileges of the QEMU process.

A privileged user/process inside guest could use this flaw to crash the QEMU process resulting in DoS or, potentially, leverage it to execute arbitrary code on the host with privileges of the QEMU process. It has a CVSSv3 Base Score of 9.9. Updates are available for this flaw.

QEMU before 2.8 built with the Cirrus CLGD 54xx VGA Emulator support is vulnerable (CVE-2017-2620) to an out-of-bounds access issue. It has a CVSSv3 Base Score of 9.9. The issue could occur while copying VGA data in cirrus_bitblt_cputovideo. A privileged user inside guest could use this flaw to crash the QEMU process or potentially execute arbitrary code on host with privileges of the QEMU process. Users are advised to install the update and shut down all running virtual machines. Once all virtual machines have shut down, start them again for this update to take effect.

The attacker can then intercept and decrypt and/or forge and inject device messages.

Cryptographic Vulnerability in Bluetooth Implementations

https://www.kb.cert.org/vuls/id/304725

Bluetooth firmware or operating system software drivers may not sufficiently validate elliptic curve parameters used to generate public keys during a Diffie-Hellman key exchange, which may allow a remote attacker to obtain the encryption key used by the device. The attacker can then intercept and decrypt and/or forge and inject device messages. Both Bluetooth low energy (LE) implementations of Secure Connections Pairing in operating system software and BR/EDR implementations of Secure Simple Pairing in device firmware may be affected. Since the vulnerability was identified, the Bluetooth SIG has updated the Bluetooth specifications to require validation of any public key received as part of public key-based security procedures, thereby providing a remedy to the vulnerability from a specification perspective. Affected users should check with their device vendor for availability of updates.

Attackers can exploit this by injecting their own namespace as a parameter in an HTTP request.

Remote Code Execution Flaw in Apache Struts 2

https://cwiki.apache.org/confluence/display/WW/S2-057

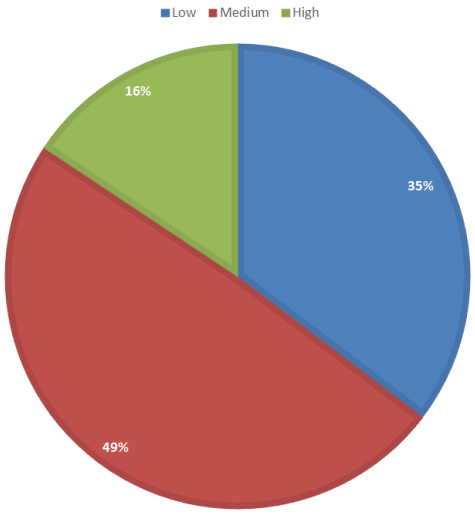
Apache Struts versions 2.3 to 2.3.34 and 2.5 to 2.5.16 suffer from possible Remote Code Execution Flaw (CVE-2018-11776). This flaw is the result of improper validation of trusted user data. Exploitation occurs when 'alwaysSelectFullNamespace' is true (either by user or a plugin like Convention Plugin) and then results are used with no namespace and in same time, its upper package has no or wildcard namespace and similar to results, same possibility when using 'url' tag which doesn't have value and action set and in same time, its upper package has no or wildcard namespace.

Attackers can exploit this by injecting their own namespace as a parameter in an HTTP request. It is recommended to upgrade to struts 2.3.35 or struts 2.5.17.

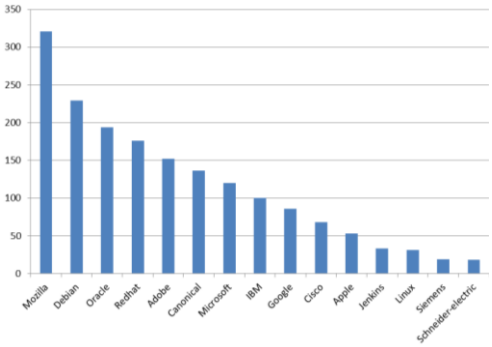
Quarterly (June-August) Vulnerability Analysis Report

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

A total of 4987 vulnerabilities have been observed in the quarter of June-August 2018. Most vulnerability was reported in July with count of 2174. The medium severity vulnerabilities are most with count of 2443. Maximum vulnerabilities have a score between 0-1 which is 1490 while 1263 vulnerabilities have been reported with score of 5-6. During this period, maximum vulnerabilities were reported in Mozilla with a count of 321 followed by Debian, Oracle, RedHat and Adobe.



Severity	CVSSv2 Score	Number of Vulnerabilities			Total Vulnerabilities	Total
		Jun	Jul	Aug		
Low	0-1	3	475	1012	1490	1763
	1-2	25	6	2	33	
	2-3	35	43	-	78	
	3-4	60	102	-	162	
Medium	4-5	357	329	4	690	2443
	5-6	535	727	1	1263	
	6-7	287	201	2	490	
High	7-8	290	192	2	484	781
	8-9	5	9	-	14	
	9-10	191	90	2	283	
Total		1788	2174	1025		4987



Security App

More than 50 percent of Facebook's Internet traffic is now secured with TLS 1.3. It is believed it is the largest deployment of TLS 1.3 — and early (0-RTT) data — on the Internet.

Facebook Released Open Source Library Fizz for TLS 1.3

https://code.fb.com/networking-traffic/deploying-tls-1-3-at-scale-with-fizz-a-performant-open-source-tls-library/

The new generation of Transport Layer Security (TLS 1.3) incorporates several new features that make Internet traffic more secure and faster than TLS 1.2. To implement TLS 1.3 Facebook has built Fizz, a library written in C++ 14. In addition to the protocol enhancements that come with TLS 1.3, Fizz offers a number of implementation features. Facebook has deployed Fizz and TLS 1.3 globally in its mobile apps, Proxygen, load balancers, internal services, and QUIC library, mvfst. More than 50 percent of Facebook's Internet traffic is now secured with TLS 1.3. It is believed it is the largest deployment of TLS 1.3 — and early (0-RTT) data — on the Internet. Fizz has reduced not only the latency but also the CPU utilization of services that perform trillions of requests a day. Every day, more than a billion people use Facebook to connect with their friends and family — and TLS 1.3 secures their data in transit from apps to servers. Facebook has open-sourced Fizz to help speed up deployment of TLS 1.3 across the Internet and help others make their apps and services faster and more secure. Fizz is built with security in mind from the ground up, with secure abstractions. The work on Fizz helped standardize the TLS 1.3 RFC.

VPNFilter Checker can help users detect the malware in their routers at work and at home.

Symantec Free Online Tool to Determine VPNFilter Malware

http://www.symantec.com/filtercheck/

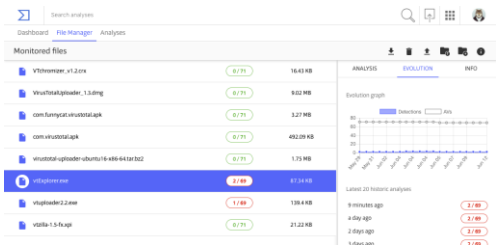
Symantec has unveiled VPNFilter Check, a free online tool designed to help individuals and organizations to determine if a router may be impacted by VPNFilter malware. VPNFilter Checker can help users detect the malware in their routers at work and at home. VPNFilter (ssler plugin) is an IoT botnet that has infected more than 500,000 consumer routers and network attached storage hardware from Linksys, Netgear, MikroTik, TP-Link and Qnap. VPNFilter can collect confidential information and tamper with network traffic as it passes through an infected router, as well as render the router unusable. The malware can also survive a reboot of the router. The tool looks at whether SSL traffic is impacted by the ssler plugin it also gives guidance on what to do if the tool does detect the plugin.

VirusTotal's New Service to Help Reduce Malware False Positives

https://blog.virustotal.com/2018/06/vtmonitor-to-mitigate-false-positives.html

VirusTotal announced a new Monitor service that helps to reduce malware false positives in software.

VirusTotal has enabled developers and antivirus vendors to check files against malware detection engines. Software developers can now benefit from a private system where they can upload new files and have them continuously checked to see if they will be flagged as malware. False positives are nothing but the virus scan results which wrongly indicate that a certain program or application is harmful or is affected by a virus. Due to the false positive results, the antivirus program may also block the program or application from running smoothly on the computer. Hence, it is necessary that there are less or no false positive results. VirusTotal Monitor program was focused on helping the antivirus industry flag malicious files. Now, the updated version of this program helps the antivirus programs to fix mistaken detections of legit files, i.e., false positives.

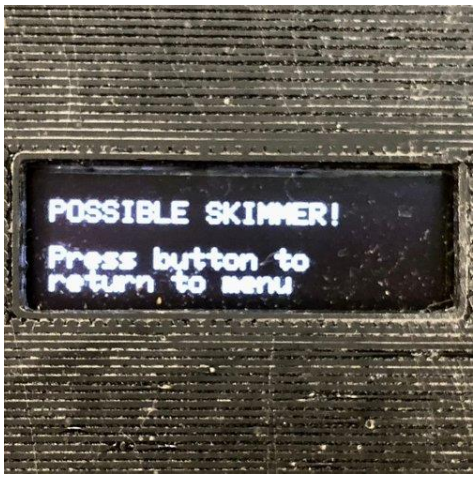


Software vendors use a Google-drive like interface where they can upload their software collections and provide details about the files

A Device that can Detect Payment Card Skimming Devices

https://www.cise.ufl.edu/~traynor/reaper/

University of Florida has developed a device that can detect different types of payment card skimming devices developed by cyber-criminals to collect data from credit and debit cards inserted inside ATMs and point-of-sale system. Skim Reaper does this with the help of a so-called 'measurement card' that a user can insert into a ATMs. With the help of an attached microcontroller, the measurement card detects the number of read heads as the card enters the ATMs. If it detects one, the ATM is deemed safe. If there are two, this means a skimmer is present. Skim Reaper is better than existing Bluetooth based solutions.



NCIIPC Initiatives

One Day Workshop on CII Protection for the Officers of Haryana

Government of Haryana organised a 'One Day Information Security Sensitization Workshop on CII Protection' for the officers of Haryana State on 27th July 2018 at Haryana Niwas, Chandigarh. The keynote address was delivered by Sh. Vijayendra Kumar, Secretary to Government of Haryana. Dr. Ajeet Bajpai, DG NCIIPC delivered talk on emerging threats and various techniques used by hackers/crackers for exploitation of sensitive installations. During this one-day event, following talks were delivered by NCIIPC:

- NCIIPC – Roles, Responsibilities and Services
- Mapping of Attack Vectors to NCIIPC Control Guidelines
- Cyber Hygiene and Best Practices
- NCIIPC SOPs for Protection of CIIs

'One Day Information Security Sensitization Workshop on CII Protection' for the officers of Haryana State on 27th July 2018 at Haryana Niwas, Chandigarh

Workshop on CII Protection for Senior Officers of Punjab Police

The workshop was inaugurated by Sh. V K Bhawra, DGP Punjab.

Punjab Police in collaboration with NCIIPC organised 'Information Security Sensitization workshop on CII Protection' for senior officers on 16th August 2018 at Punjab Police Head Quarters, Chandigarh. The workshop was inaugurated by Sh. V K Bhawra, DGP Punjab. The workshop started with talk by Director NCIIPC and officers on 'Roles and Responsibilities of NCIIPC to protect the National Critical Information Infrastructure' followed by hands-on session on 'Cyber Hygiene and Best Practices'. The session was concluded with a talk on NCIIPC SOPs for Protection of CIIs.

The Cyber Security Training Centre was inaugurated by Hon'ble Chief Minister of Uttarakhand on 9th July 2018 at Dehradun.

Establishment of Cyber Security Training Centre at Uttarakhand

With an objective to improve cyber hygiene at work place and at State's Critical Information Infrastructure, Government of Uttarakhand has established a Cyber Security Training Centre in coordination with Information Technology Development Agency (ITDA) and NCIIPC. The Cyber Security Training Centre was inaugurated by Hon'ble Chief Minister of Uttarakhand on 9th July 2018 at Dehradun.

NCIIPC Responsible Vulnerability Disclosure Program

http://nciipc.gov.in/RVDP.html

NCIIPC acknowledges the researchers for their contributions towards protection of National Critical Information Infrastructure.

The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in nation's Critical Information Infrastructure. NCIIPC acknowledges the following researchers for their contributions towards disclosure of vulnerabilities for protection of National Critical Information Infrastructure:

- Sh. Aksh Labade
- Sh. Akshay
- Sh. Dhananjay Garg
- Sh. Pappu Mandal
- Sh. Shubham Khandgi
- Sh. Adesh Kolte
- Sh. Aman Sethi
- Sh. Aagam Shah
- HackersEra VMS

Upcoming Events - Global

October 2018

- ISC2 Secure Summit, Toronto 1 Oct
- Oil & Gas Cybersecurity Summit & Training, Houston 1-6 Oct
- Cyber Security for Critical Assets, London 2-3 Oct
- AppSec USA, San Jose 8-12 Oct
- Annual Industrial Control Cyber Security, London 9-10 Oct
- ATM & Cyber Security, London 9-10 Oct
- International Conference on Security of Smart Cities, Industrial Control System and Communications, Shanghai 18-19 Oct
- ICS Cyber Security Conference, Atlanta 22-25 Oct
- International Summit on Cyber Security in SCADA and Industrial Control Systems, Stockholm 22-25 Oct
- Cybersecurity for Industrial Environments and Critical Infrastructures, Manchester 23-25 Oct
- ACS/IEEE International Conference on Computer Systems and Applications, Aqaba 28 Oct - 1 Nov
- US China Blockchain and Digital Currency Conference, Las Vegas 30 Oct

OCTOBER 2018

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 2018

- International Workshop on Intelligent Devices and Information Security for Transportation Systems, Maui 4-7 Nov
- Annual Aviation Cyber Security Summit, London 6-7 Nov
- IFINSEC Financial Sector IT Security Conference and Exhibition, Istanbul 13-14 Nov
- INext Generation Cyber Ranges, Athens 18-22 Nov
- International Workshop on the Security of Video Surveillance Systems, Auckland 27-30 Nov

NOVEMBER 2018

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	

December 2018

- Annual Industrial Control System Security Workshop, San Juan 4 Dec
- Intel Security Conference, Hillsboro 4-5 Dec
- International Conference on Network Security Taipei 14-16 Dec

January 2019

- Cyber Security for Critical Assets, Dubai 21-22 Jan

DECEMBER 2018

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 2019

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		

Upcoming Events - India

- c0c0n, Kochi 5-6 Oct
- HAKON - International Information Security Meet Indore 7 Oct
- First International Conference on Secure Cyber Computing and Communication, Jalandhar 11-13 Oct
- International Conference on Cyber Security, Jaipur 26-27 Oct
- SANS Mumbai 2018 12-17 Nov
- International Conference on Cyberlaw, Cybercrime & Cybersecurity, New Delhi 14-16 Nov
- 21st Association of Anti-Virus Asia Researchers Conference 2018, Goa 28-30 Nov
- Cyber Security India, Hyderabad 4-5 Dec
- SPACE 2018 — Conference on Security, Privacy and Applied Cryptography Engineering, Kanpur 17-19 Dec
- SANS Bangalore 2019 7-19 Jan
- SANS Secure India 2019, Bangalore 4-9 Mar

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

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.