NEWSLETTER

July 2017

National Critical Information Infrastructure Protection Centre

VOLUME 1 ISSUE 3

NCIIPC Newsletter

July 2017

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

Welcome to the third issue of NCIIPC quarterly newsletter. We hope this initiative is helping you gain insights into the current trends in cyber security.

The last quarter has seen raising awareness among the world community for urgent implementation of cyber security mechanisms. 'WannaCry' ransomware, which affected around 2 lakh computers across 150 nations, has shown that vulnerabilities and malwares have no boundaries and can damage small businesses, big corporates and governments, alike. Revelations of NSA hacking tools have shown the potential threats posed by undisclosed vulnerabilities and exploits and the extent of damage that can be caused. Consequent to emerging cyber threats such as these, Govt. of India, inter-alia, has taken new and focused initiatives to mitigate them by creating separate CERTs for financial and power sectors.

NCIIPC conducted various programs to sensitize employees dealing with critical information infrastructure. A one day workshop was organised at UIDAI to bring the awareness about various cyber threats and role of NCIIPC. A program with the Delhi Govt. was also organised to bring awareness about WannaCry ransomware. NCIIPC in collaboration with Independent Power Producers Association of India (IPPAI) organised a one day workshop on implementation of cyber security in power infrastructure. NCIIPC is actively engaged with various CII organisations for identification of critical information assets.

We request the readers to provide their valuable suggestions/feedbacks for improvement. Readers may also contribute any relevant information/article for this newsletter. You may write to us at newsletter@nciipc.gov.in.

News Snippets - National

Indian Systems Largely Escape Global Ransomware Attack

Source: Firstpost

Indian computer systems largely escaped the global ransomware attack as government and private establishments had by and large installed timely critical security updates to mitigate the unrivalled global cyber-attack.

Over two lakh computers in at least 150 countries are said to have been infected. However, in India, only a few isolated incidents in West Bengal, Kerala, Andhra Pradesh and Tamil Nadu were reported. CERT-In issued a list of do's and don'ts and organized a webcast on how to protect networks from the global ransomware attack. Automaker Nissan, which saw its systems being impacted globally, said the Renault-Nissan alliance plant in Chennai did come under attack, but its India team had responded well to avoid major impact on the business. Most importantly, GSTN, the company set up to provide the IT infrastructure for GST rollout, was not impacted by the WannaCry ransomware attack as its systems do not run on Microsoft software.

CERT-In advisory on WannaCry Ransomware

Separate CERT for Financial and Power Sectors

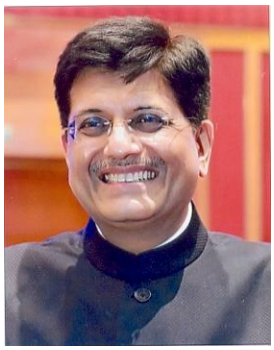
Source: Business Standard

The Central Govt. is planning to set up separate cyber security teams for different sectors in the face of emerging cyber threats such as the recent ransomware attack. A centralised hub to monitor and take on such attacks is also on the agenda. Minister for IT, Sh. Ravi Shankar Prasad, said that the govt. was planning to set up separate Indian Computer Emergency Response Teams for the financial and power sectors to deal with specific cyber threats.

A separate CERT for the financial sector and a dedicated digital payment division will ensure and secure the digital payments ecosystem. GoI has also issued directives to banks to conduct routine technology audits. It is setting around 10 standardisation testing and quality certification centers, in Jammu and Kashmir, Uttarakhand, Chattisgarh, Bihar and Jharkhand. It will also work with private firms to reinforce cyber security of different areas. Cyber security drills and auditing for assessment of security preparedness of organisations are being done. The Centre has approved an outlay of Rs. 100 crore for a project to clean botnets on real time basis.

IT Minister Sh. Ravi Shankar Prasad

A separate CERT for the financial sector and a dedicated digital payment division will ensure and secure the digital payments ecosystem.



Union Minister of State for Power, Coal, New & Renewable Energy and Mines Sh. Piyush Goel

Four Sectoral CERTs, CERT (Transmission), CERT (Thermal), CERT (Hydro) and CERT (Distribution) have been formed.

Four Sectoral CERTs to Mitigate Threats in Power Systems

Source: Business Standard

Government of India, in line with National Cyber Security Policy 2013, has created sectoral Computer Emergency Response Teams (CERTs) to mitigate cyber security threats in power systems. Union Minister of State for Power, Coal, New & Renewable Energy and Mines informed that Government of India through Ministry of Electronics & Information Technology and National Critical Information Infrastructure Protection Centre has taken several steps to make key stakeholders of the power sector aware, and take precautions against cyber threats. The Minister added that for cyber security in power systems, four Sectoral CERTs, CERT (Transmission), CERT (Thermal), CERT (Hydro) and CERT (Distribution) have also been formed to coordinate with power utilities. The relevant stakeholders of Smart Grid have been advised to identify critical infrastructure and use end-to-end encryption for data security. All utilities have been asked to identify a nodal senior executive as its Chief Information Security Officer to lead the process of strengthening organizational systems with respect to cyber security, and implement an Information Security Management System as recommended by rules framed under the Information Technology (IT) Act 2008.

News Snippets - International

WannaCry affected over 200000 computer systems in at least 150 nations. Photo credit: AFP

British IT expert Marcus Hutchins has been branded a hero for slowing down the WannaCry global cyber-attack. (Photo: AP)

WannaCry Affected 200000 Computers in 150 Nations; Govts. Alerted Against Cyber Attacks More Dangerous than WannaCry

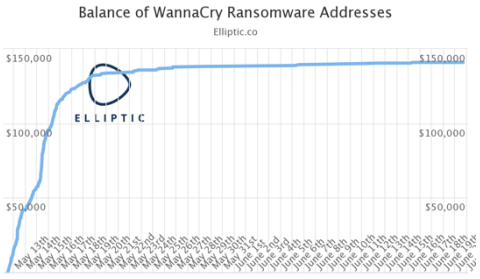
Source: BBC, Scroll.in

WannaCry, the ransomware used for a global cyber-attack on May 12 2017, affected over 200000 computer systems in at least 150 nations. The attackers, apparently, raked in over $1 million in the digital currency Bitcoin from their victims. A majority of machines hit by the WannaCry ransomware were running Windows 7. Many organisations seem to have been caught out because they failed to apply a patch, issued by Microsoft in March that blocked the vulnerability which WannaCry exploited. Spanish telecoms firm Telefonica, French carmaker Renault, German rail firm Deutsche Bahn, logistics firm FedEx, Russia's Interior Ministry and 61 NHS organisations were all caught out by WannaCry. After encrypting files, the WannaCry demanded a payment of $300 in bitcoins before they were unfrozen. There have been no reports that anyone who paid has had their data restored. A 22-year-old researcher named Marcus Hutchins helped slow the malware's spread by discovering, and then registering, a domain name inside its code.

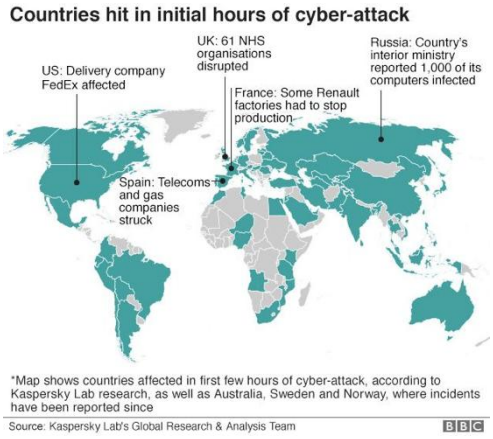
Cyber security researchers around the world have said they have found evidence that could link North Korea with the WannaCry cyber-attack. Some code in an earlier version of the WannaCry software had also appeared in programs used by the Lazarus Group, identified by some researchers as a North Korea-run hacking operation.

Indian Government alerted the users against potential cyber-attacks with two pieces of malware that are likely more dangerous than WannaCry. The new threats have been identified as 'Adylkuzz' and 'EternalRocks'. While Adylkuzz uses two exploits like WannaCry, EternalRocks leverages all seven exploits stolen from the United States National Security Agency and dumped online by the Shadow Brokers hacker group. "Adylkuzz is a cryptocurrency miner that exploits vulnerability in the Windows operating system just like WannaCry to generate digital cash," said the first alert issued by the NCIIPC on May 25. "Unlike WannaCry, which locks down a system until ransom is paid; Adylkuzz allows the computer to work but at the same time generates digital cash or Monero cryptocurrency in the background."

In another advisory issued on May 26, the government described the second potential threat. EternalRocks is a new Network Worm which is the successor to the WannaCry ransomware. EternalRocks leverages some of the same vulnerabilities and exploit tools as WannaCry but is potentially more dangerous because it exploits seven NSA tools that were released as part of the Shadow Brokers dump for infection instead of two used by WannaCry. EternalRocks has the potential to spread faster and infect more systems. EternalRocks is currently dormant and is not doing anything nefarious such as encrypting hard drives. But EternalRocks could be easily weaponised in an instant, making the need for preventive action urgent. The twin alerts were put out on the centre's website and the Cyber Swachhta Kendra's as well. The government has listed a few precautionary measures in its advisories. These include making regular data backups, enabling visibility of hidden file extensions, installing regular updates and patches, avoiding opening of unsolicited attachments and enabling the Windows firewalls.



Total ransomed: $132,161.73. Up to: June 28th, 10:57 AM



Indian Government alerted the users against potential cyber-attacks with two pieces of malware that are likely more dangerous than WannaCry.

SMB Vulnerabilities being used to Distribute Trojan Malware

Source: zdnet.com

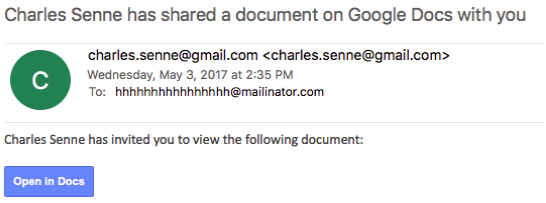
Leaked NSA exploits which helped the WannaCry ransomware outbreak become so prolific is now being used to distribute Trojan malware.

Those behind this new Gh0st RAT campaign are using EternalBlue exploits in an effort to compromise Singapore, while Nitol is attacking the wider South Asia region.

The SMB vulnerabilities are being used to distribute Backdoor.Nitol - a Trojan horse which opens a backdoor on the infected computer - and Gh0st RAT, a form of malware capable of taking full control of a machine in addition to conducting espionage and stealing data. The latter is particularly dangerous and is repeatedly a thorn in the side of the aerospace and defense industries, as well as government agencies. Those behind this new Gh0st RAT campaign are using EternalBlue exploits in an effort to compromise Singapore, while Nitol is attacking the wider South Asia region. The initial exploit used at the SMB level is similar to what's been seen in WannaCry attacks, but instead of being used to deploy ransomware, the attack opens a shell to write instructions into a VBScript file which is when executed to retrieve the payload from another server in order to create the required backdoor into the machine using Nitol or Gh0st RAT. While neither attack is new - both have plagued victims for years – the use of EternalBlue provides additional potency to attacks.

End users should beware of clicking on links in emails from strangers or opening email attachments.

Note: Server Message Block (SMB) is the protocol used by Windows for file/printer sharing and access to remote Windows services. SMB operates over TCP ports 139 and 445. As a precautionary measure, users should backup data on regular basis and update software including antivirus software. End users should beware of clicking on links in emails from strangers or opening email attachments.



An e-mail where it appears that a user (potentially even one on your contact list, so it looks very legitimate) has shared a document. Source: https://isc.sans.edu/

1mn Gmail Users Victimized by Google Docs Phishing Scam

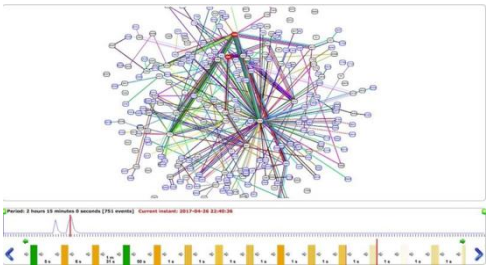
Source: threatpost.com

Up to 1 million Gmail users were victimized by Google Docs phishing scam that spread quickly for a short period of time. Google took measures to protect its users by disabling offending accounts, and removing phony pages and malicious applications involved in the attacks. Other security measures were pushed out in updates to Gmail, Safe Browsing and other in-house systems. The messages were a convincing mix of social engineering and abuse of users' trust in the convenience of mechanisms that share account access with third parties. Many of the phishing messages came from contacts known to victims since part of the attack includes gaining access to contact lists. The messages claimed that someone wanted to share a Google Doc with the victim, and once the "Open in Docs" button in the email is clicked, the victim is redirected to a legitimate Google OAUTH consent screen where the attacker's application, called "Google Docs" asks for access to victim's Gmail and contacts through Google's OAUTH2 service implementation.

Network Traffic of 36 Large Network Blocks Routed Through Russia

Source: arstechnica.com

On 26th April, large chunks of network traffic belonging to MasterCard, Visa, and more than two dozen other financial services companies were briefly routed through a Russian telecom. While it's possible that this 5 to 7 minutes hijack of 36 large network blocks may have been inadvertent, the high concentration of technology and financial services companies affected made the incident "curious" to engineers at network monitoring service BGPmon. The way some of the affected networks were redirected indicated their underlying prefixes had been manually inserted into BGP tables (Routing protocol among Internet backbones, ISPs, and other large networks), most likely by someone at Rostelecom, the Russian controlled telecom that improperly announced ownership of the blocks. The hijacking could have allowed individuals in Russia to intercept or manipulate traffic flowing into the affected address space. Such interception or manipulation would be most easily done to data that wasn't encrypted. The affected company networks also included those belonging to security provider Symantec and technology company EMC.

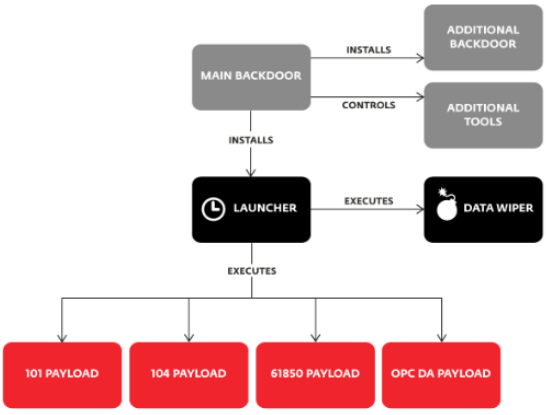


A map visualizing network changes being announced by Rostelecom.

Industroyer or Crashoverride to Harm Critical Infrastructure

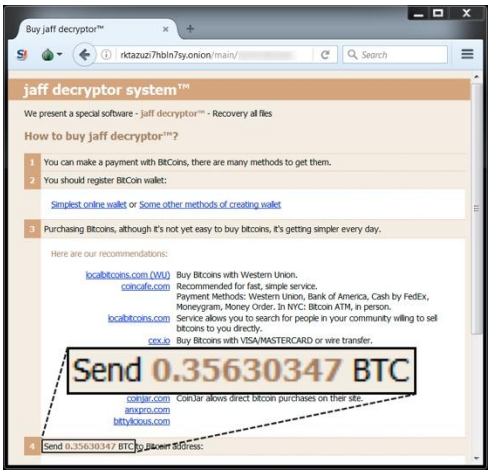
Source: voanews.com

Two cybersecurity firms said that they have uncovered malicious software that they believe caused the December 2016 Ukraine power outage, warning that the malware could be easily modified to harm critical infrastructure operations around the globe. ESET, a Slovakian anti-virus software maker, and Dragos Inc., a U.S. critical infrastructure security firm, released detailed analyses of the malware, known as Industroyer or CrashOverride. The security firms warned that there could be more attacks using the same approach, either by the group that built the malware or copycats who modify the malicious software. It is capable of causing outages of up to a few days in portions of a nation's grid, but is not potent enough to bring down a country's entire grid. With modifications, the malware could attack other types of infrastructure including local transportation providers, water and gas providers. CrashOverride can be detected if a utility specifically monitors its network for abnormal traffic, including signs that the malware is searching for the location of substations or sending messages to switch breakers.



It is capable of causing outages of up to a few days in portions of a nation's grid, but is not potent enough to bring down a country's entire grid.

Trends



Victims must open the PDF attachment, agree to open the embedded Word document, and then enable macros on the embedded Word document to infect their Windows computers.

Jaff Ransomware

Source: isc.sans.edu

Since 11th May 2017, a new ransomware named "Jaff" has been distributed through malicious spam (malspam) from the Necurs botnet. This malspam uses PDF attachments with embedded Word documents containing malicious macros. Victims must open the PDF attachment, agree to open the embedded Word document, and then enable macros on the embedded Word document to infect their Windows computers. Prior to Jaff, waves of malspam using the same PDF embedded Word doc scheme to push Locky ransomware and Dridex were seen. This specific wave of malspam used a fake invoice theme. The embedded macros generate an initial URL to download an encoded Jaff binary, and then another URL for post-infection callback from an infected host. The initial HTTP request for Jaff returns an encoded binary that's been XORed with the ASCII string I6cqcYo7wQ. The encoded binary from this wave of malspam was stored to the user's AppData\Local\Temp directory as lodockap8. Then it was decoded and stored as levinsky8.exe in the same directory. These file names change everyday with each new wave of malspam. Much of this malspam is easy to spot among the daily deluge of spam most organizations receive. However, this PDF attachment/embedded Word doc scheme is likely an attempt to bypass spam filtering.

Implementing BGP Route Origin Validation based upon the Resource Public Key Infrastructure can mitigate accidental and malicious attacks associated with route hijacking.

Secure Inter-Domain Routing

Source: nccoe.nist.gov

Since the creation of the Internet, Border Gateway Protocol (BGP) has been the default routing protocol to route traffic among organizations (Internet Service Providers (ISPs) and Autonomous Systems (ASs)). While the BGP protocol performs adequately in identifying viable paths that reflect local routing policies and preferences to destinations, the lack of built-in security allows the protocol to be exploited. As a result, attacks against Internet routing functions are a significant and systemic threat to Internet based information systems. To improve the security of inter-domain routing traffic exchange, NIST has begun development of a special publication that provides security recommendations for the use of Inter-domain protocols and routing technologies. These recommendations aim to protect the integrity of internet traffic exchange. Implementing BGP Route Origin Validation (ROV) based upon the Resource Public Key Infrastructure (RPKI) can mitigate accidental and malicious attacks associated with route hijacking. The NCCoE recently released a draft project description Secure Inter-Domain Routing: Route Hijacks.

Hajime Neutralising Mirai Botnet

Source: bleepingcomputer.com

```
Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!
```

Hajime, an IoT malware discovered last October, appears to be the work of a vigilante who has set out to take over and neutralize as many smart devices as possible before other botnets like Mirai can get a hold of them. It only recently became apparent to researchers that the author of this malware had no intention of using infected devices for evil. Hajime came with a self-replication module that allowed it to spread from IoT device to device via open and unsecured Telnet ports. The malware's author didn't add a DDoS feature, didn't use his botnet to relay malicious traffic, or any other intrusive operation. Once Hajime infects a device it blocks access to ports 23, 7547, 5555, and 5358, which are all ports that have been exploited in the past by IoT malware. After that, Hajime contacts its command and control server and returns a cryptographically-signed message every ten minutes. This tactic appears to have been a success as Hajime spread quickly across the globe, already taking over and neutralizing a large number of devices in countries such as Brazil, Iran, and Russia.

The author of this malware had no intention of using infected devices for evil.

Note: Mirai is a malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices. The default settings of the devices should be changed to prevent your device to be part of botnet.

Ransomware as a Service: New Challenge to Cyber Security

Source: thehackernews.com

Cyber Ransomware has become an albatross around everyone's neck, targeting businesses, hospitals, financial institutions and individuals worldwide and extorting millions of dollars. Ransomware as a Service (RaaS) is a variant of ransomware designed to be so user friendly that anyone with little or no technical knowledge can also easily deploy them to make money. Russian Hackers are selling cheap Ransomware as a Service on Dark Web. Security researchers have uncovered an easy to use ransomware service that promises profit with just one successful infection. Dubbed 'Karmen', the RaaS variant is based on the abandoned open source ransomware building toolkit dubbed Hidden Tear and is being sold on Dark Web forums from Russian speaking hacker named DevBitox for $175. Like any typical ransomware infections, Karmen encrypts files on the infected PC using the strong AES-256 encryption protocol, making them inaccessible to the victim until he/she pays a large sum of money to obtain the decryption key from the attacker.

Karmen automatically deletes its decryptor if a sandbox environment or analysis software is detected on the victim's computer to keep security researchers away from investigating the threat.

This new variant of ransomware as a service provides buyers' access to a web based control panel hosted on Dark Web with a user friendly graphical dashboard that allows buyers to configure a personalised version of the Karmen ransomware. The dashboard lets buyers keep a running tally of the number of infections and their profit in real time, allowing anyone with very minimal technical knowledge to deploy Karmen, threat intelligence firm Recorded Future said in a blog post. Once infected, the Karmen ransomware encrypts the victim's files and shows a popup window with a threatening message warning users not to interfere with the malware; otherwise, they might lose all their files. What's more interesting? Karmen automatically deletes its decryptor if a sandbox environment or analysis software is detected on the victim's computer to keep security researchers away from investigating the threat. Initial Karmen infections were reported in December 2016 by victims in Germany and the United States, while the sale in underground forums began in March 2017.

Learning

Establishing ICS Security Operation Centre (SOC)

The scope of the SOC should not be limited to an IT Department of the organization; it should extend to encompass OT/ICS infrastructure as well.

Sh. Mohd. Zaki Ahmed, Sectoral Coordinator (Power & Energy), zaki@nciipc.gov.in

With the convergence of Information Technology (IT) and Operations Technology (OT), critical sectors such as Power & Energy are relying more and more on Industrial Control Systems (ICS) to manage and operate their critical business processes. Usage of ICS is enabling organizations to operate their business processes more efficiently and to provide new functionalities. ICS systems may include SCADA (Supervisory Control and Data Acquisition) system and/or Distributed Control Systems (DCS) for centralized and/or distributed control of management of processes. To attain situational awareness and the capability to forecast & mitigate cyber threats, organizations are recommended to establish Security Operation Centre (SOC). However, as OT is a major concern for the organizations discussed here, the SOC should be an "ICS SOC" kind. The scope of the SOC should not be limited to an IT Department of the organization; it should extend to encompass OT/ICS infrastructure as well. The following points may be considered while establishing the ICS SOC:

- Analysis Team of SOC should have expertise to monitor and analyse ICS logs for cyber threats.
- A Policy for incident handling along with escalation matrix should be developed. Contact details of all relevant officials from OT should be available with SOC team.

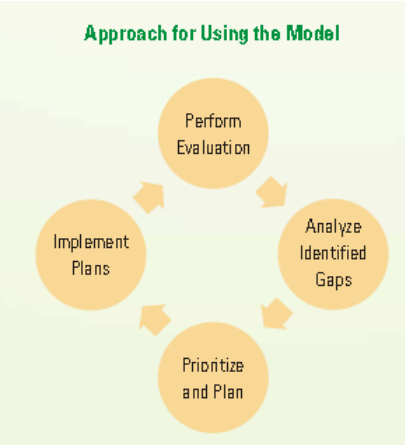
- Because of interdependency, an incident may cause cascading impact on other organizations. For example, an incident to Power Transmission utility may affect operations of Power Distribution utility, and an incident on upstream organization of Energy Sector may cause adverse effects to operations of downstream organizations. Mechanisms of Information Sharing in respect of cyber security incidents should be established with all those organization on which there is any interdependency.
- The SOC should also play an active role in monitoring access of vendors/service-providers to OT systems. Usage of un-trusted/un-authorised portable media such as USB or connectivity of Laptop or equipment's to the ICS network must be avoided.
- SOC should be able to collect logs from Human-Machine interface (HMI), Programmable Logic Controllers (PLC), Intelligent Electronic Devices (IED), Remote Terminal Units (RTU), Distributed Control Systems (DCS), SCADA etc.
- ICS devices such as PLCs have a very static pattern of communication over DNP/MODBUS/ICCP. Any abnormal pattern such as a device trying to connect with unknown IP addresses should be monitored and incident alert should be issued on priority.

Any abnormal pattern such as a device trying to connect with unknown IP Addresses should be monitored and incident alert should be issued on priority.

Cybersecurity Capability Maturity Model (C2M2)

Source: indiasmartgrid.org

In the present era, there is a dire need for improved cyber security as repeated cyber intrusions pose serious threats to organizations. Cyber threats continue to grow, and represent one of the most serious operational risks facing modern organizations. The national and economic security of a nation depends upon the reliable operation of the Nation's critical infrastructure in the face of such threats. The Cybersecurity Capability Maturity Model (C2M2) can help organizations of all types, sizes and sectors assess their cyber security assets and practices in order to help them make improvements to their cyber security programs. C2M2 has been developed by United States Department of Energy by removing its sector-specific references and terminology. The C2M2 emphasizes on the implementation and management of cybersecurity practices associated with the Information Technology (IT) and Operations Technology (OT) assets and the environments in which they operate.



Summary of Maturity Indicator Level Characteristics

Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial Practices are performed but may be adhoc
MIL2	*Institutionalization characteristics* • Practices are documented • Stakeholders are identified and involved • Adequate resources are provided to support the process • Standards or guidelines are used to guide practice implementation *Approach characteristic* • Practices are complete or advanced than at MIL1
MIL3	*Institutionalization characteristics* • Activities are guided by policies(or other directives) and governance • Policies include compliance requirements for specified standards or guidelines • Activities are periodically reviewed to conformance to policy • Responsibility and authority for practices are assigned to personnel Personnel performing the practice have adequate skills and knowledge *Approach characteristic* • Practices are complete or advanced than at MIL1

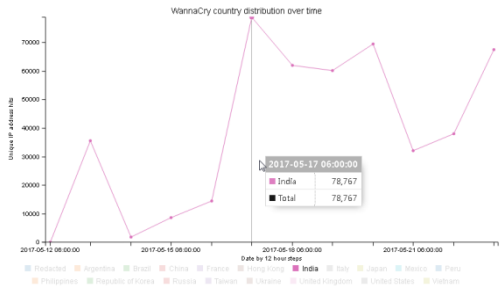
The audiences that may benefit from C2M2 are decision makers who control the resource allocation in the organisation, leaders who manage resources and operations, practitioners responsible for planning and managing organisational changes and various facilitators leading to self-evaluation of organisation based on C2M2. Maturity Indicator Levels or the MILs form the backbone of C2M2 which indicate to the organisation their present state situation and their aspirations/ future state situation with regards to cybersecurity domain. There are 4 Maturity Indicator Levels, MIL0 through MIL3, which individually apply to each domain in the model. The C2M2 is meant to be used by an organization to evaluate its cybersecurity capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments. An organization performs an evaluation against the model, uses that evaluation to identify gaps in capability, prioritizes those gaps, develops plans to address them, and finally implements those plans to address the gaps. The C2M2 is an effective tool for the organisations to combat their cybersecurity challenges. C2M2 provides a powerful and concrete means to evaluate and mitigate an organisation's cybersecurity capabilities and challenges in order to help them assess their current situation and devise appropriate defensive systems.

WannaCry Working Summary

Source: isc.sans.edu, us-cert.gov

At the time of initial WannaCry outbreak, a significant increase in scanning for port 445 was also noticed.

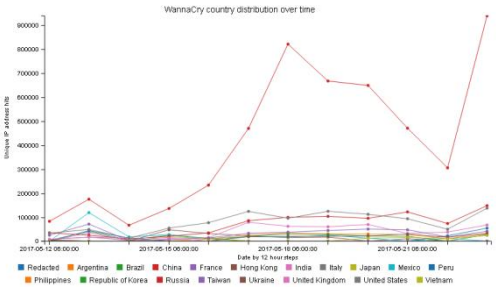
The WannaCry ransomware spread very quickly throughout the world. This sample used the SMBv1 ETERNALBLUE exploit to spread. ETERNALBLUE became public as part of Shadowbroker archive of NSA hacking tools. A month prior to release of the hacking tool, Microsoft patched the vulnerability as part of the March Patch Tuesday release. The patch was released for all supported versions of Windows as part of MS17-010. In response to the rapid spread of WannaCry, Microsoft released a patch for unsupported versions of Windows, i.e. Windows XP and Windows Server 2003. At the time of initial WannaCry outbreak, a significant increase in scanning for port 445 was also noticed. The increase was likely caused by infected systems scanning for more victims.



Spread of WannaCry in India
Source: blog.kryptoslogic.com

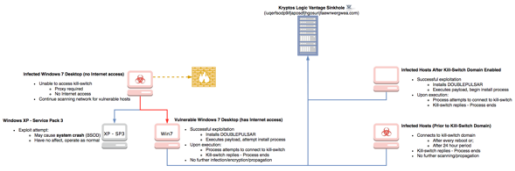
The malware first checks if it can reach a specific website at http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. It also checks if a registry key is present. It will not run if either the registry key is present or the website is reachable. A tool "Tearst0pper" was released by Rendition InfoSec that assists in setting the registry keys, which also reduce the risk of infection.

The malware is designed to run as a service with the parameters "-m security". During runtime, the malware determines the number of arguments passed during execution. If the arguments passed are less than two, the dropper proceeds to install itself as mssecsvc2.0 service. Once the malware starts as a service, the dropper attempts to create and scan a list of IP ranges on the local network and attempts to connect using UDP ports 137, 138 and TCP ports 139, 445. If a connection to port 445 is successful, it creates an additional thread to propagate by exploiting the SMBv1 vulnerability. The malware then extracts and installs a PE32 binary from its resource section named "R". This binary has been identified as the ransomware component of WannaCrypt. The dropper installs this binary into C:\WINDOWS\tasksche.exe and executes the same.



Spread of WannaCry in various countries. China is the worst hit. Source: blog.kryptoslogic.com

The malware creates a 2048 bit RSA key pair. The private key is encrypted using a public key that is included with the malware. For each file, a new random AES key is generated. This random AES key is then encrypted using the public user key. To decrypt the files, the user's private key needs to be decrypted, which requires the malware author's private key? Unlike some other ransomware, no network communication is needed to generate these keys. The password "WNcry@2ol7" is not used to encrypt files. It is only used by the malware to decrypt some of its components. Encrypted files use the extension .wncry. To decrypt the files, the user is asked to pay $300, which will increase to $600 after a few days. The ransomware threatens to delete all files after a week.



Process flow of WannaCry Ransomware Source: blog.kryptoslogic.com

In addition to encrypting files, the malware also installs a DOUBLEPULSAR back door. The backdoor could be used to compromise the system further. The malware will also install Tor to facilitate communication with the ransomware author.

```
--Begin service--

ServiceName = "mssecsvc2.0"
DisplayName = "Microsoft Security
Center (2.0) Service"
StartType = SERVICE_AUTO_START
BinaryPathName = "%current
directory%5bef35496fcbdbe841c82f4
d1ab8b7c2.exe -m security"

--End service--
```

Securing Digital Footprints: E-Governance

Sh. Navdeep Pal Singh, Sectoral Coordinator (Government), coord.gov@nciipc.gov.in

The shift from paper work to digital services, for transparent, effective and timely delivery of services is proliferating the digital footprints of citizens in the cyber domain which needs to be secured at different stages. These stages can be categorized as:

Planning Stage: Planning stage ensures that security is taken as a key design parameter for all the new critical IT infrastructures at the conceptualization and design level itself.

Implementation Stage: Implementation stage caters to the requirements of Cyber Security at the deployment stage like OS hardening, Hardware testing, perimeter protection etc.

This stage also takes into cognizance the retrofitting exercise by protecting all the unprotected systems.

Operational Stage: This Operational Stage controls the Cyber Security posture of the entire IT infrastructure including networks and applications while in operational phase 365x24x7, like auditing, upgrading, updating etc.

Continuity Stage: Main aim of the stage is to maintain the resiliency of the systems against all known cyber-attack vectors, ensuring minimum MTTR (Mean Time To Recover) and maximum MTBF (Mean Time Between Failures).

Compliance Stage: This stage acts as a cop to check any incidents, abnormal behavior, logs, policy and framework compliance. Ignoring this stage can result in missing the golden window to catch the sophisticated attacks on the critical IT infrastructures at the nascent stage itself.

CISO of the organization also has the responsibility to sensitize entire staff including senior-most officials dealing with IT infrastructure with the basic Cyber Hygiene, organization expects in the form of IS policy.

Modus-operandi of the cyber-attack on the e-governance platforms had been observed to be revolving around targeting Confidentiality, Integrity and Availability (CIA) triad. It has been observed that sometimes employees are ignorant about the basic Cyber Hygiene as desired in the Information Security (IS) policy of the organization. CISO of the organization also has the responsibility to sensitize entire staff including senior-most officials dealing with IT infrastructure with the basic Cyber Hygiene, organization expects in the form of IS policy.

File-less Attacks

Sh. Ankit Sarkar, Scientist-D, NCIIPC, a.sarkar@nciipc.gov.in

https://www.hackread.com/wp-content/uploads/2017/02/the-rise-of-file-less-attacks-3-758x412.png

A file-less, or malware-free, attack occurs when an attacker evades detection by eliminating the traditional step of copying a PE (Portable Executable) file to the disk drive. There are multiple techniques to compromise a system in this fashion.

A file-less, or malware-free, attack occurs when an attacker evades detection by eliminating the traditional step of copying a PE (Portable Executable) file to the disk drive.

Exploits commonly are used to execute attacks directly in memory by exploiting vulnerabilities that exist in the operating system (OS) or in installed applications. Exploit kits have made attacking easier and more efficient by allowing automation and mass-perform initial compromises. All that is required is for a victim to be lured into an exploit kit server, often via phishing or social engineering. The kits usually provide exploits for a multitude of vulnerabilities, as well as a management console that allows the attacker to control the compromised system.

The *use of stolen credentials* is another widespread method of initiating a file-less attack.

Having *weak credentials* allow the attacker to access the system as a normal user.

Once the initial compromise is achieved, the adversary can rely on tools provided by the OS itself, such as Windows Management Instrumentation and PowerShell, to perform further actions without having to save files to disk.

Registry Resident Malware: The Malware installs itself in the Windows Registry in order to remain persistent while evading detection. The first of its kind was Poweliks, and many variants, such as Kovter, have been seen since then. Poweliks calls back to a command and control server from which the attacker can send further instructions to the compromised system. All of those actions can take place without any file being written to disk.

Memory-only malware: Some malware reside only in memory to evade detection. This is the case with Duqu worm, which can remain undetected by residing exclusively in memory. Duqu 2.0 comes in two versions; the first is a back door which allows an attacker to gain a foothold in an organization. If the target is deemed worthy by the attacker, he can then use the advanced version, which offers additional features such as reconnaissance, lateral movement and data exfiltration.

File-less ransomware: In this, malicious code is either embedded in a document, using a native scripting language such as macros, or written straight into memory using exploits. The ransomware then uses legitimate administrative tools such as PowerShell to encrypt hostage files, all without being written to disk.

Problem: File-less attack are on the rise because they are extremely hard for traditional security solutions to detect.

Legacy antivirus (AV) is designed to look for signatures of known malware. Since file-less attacks have no malware, there is nothing for AV to detect.

The whitelisting approach involves listing all the good processes on a machine, to prevent unknown processes from executing. The problem with file-less attacks is that they exploit legitimate whitelisted applications that are vulnerable.

Using indicator of compromise (IOC) tools to prevent file-less attacks is not very efficient, either. In essence, IOCs are similar to conventional AV signatures in that they are known malicious artifacts left behind by an attacker. However, because they leverage legitimate processes, and operate inside memory, file-less attack do not leave artifacts behind.

Another approach involves sandboxing, which includes network-based detonation and micro virtualization. Since file-less attacks do not use PE files, there is nothing for the sandbox to detonate. Even if something was sent to the sandbox, since file-less attacks usually hijack legitimate processes, most sandboxes would ignore it.

File-less attack are on the rise because they are extremely hard for traditional security solutions to detect.

Since file-less attacks have no malware, there is nothing for AV to detect.

They exploit legitimate whitelisted applications that are vulnerable, and they take advantage of built-in operating system executables.

Protection: To protect against stealthy, file-less attacks, multiple methods need to be combined into a powerful and integrated approach.

Application inventory discovers any applications running in an environment, helping find vulnerabilities so one can patch or update them and they can't be the target of exploit kits.

IOAs look for signs that an attack may be underway, instead of being concerned about how the steps of the attack are being executed.

Indicators of Attack (IOAs) identify and block malicious activity during the early stages of an attack, before it can fully execute and inflict damage. IOAs look for signs that an attack may be underway, instead of being concerned about how the steps of the attack are being executed. Those signs can include code execution, attempts at being stealthy and lateral movement, to name a few. IOAs are concerned with the actions performed, their relation to each other, their sequence and their dependency, recognizing them as indicators that reveal the true intentions and goals behind a sequence of events. IOAs are not focused on the specific tools and malware that attackers use. IOAs detect the sequences of events that a piece of malware or an attack must undertake to complete its mission. This exposes even the stealthiest file-less methods so they can be addressed promptly. IOAs can detect and block malicious activities, even if they are perpetrated using a legitimate account, which is often, the case when an attacker uses stolen credentials.

Managed hunting proactively searches around the clock for malicious activities that are generated as a result of file-less technique. This method ensures that even the most sophisticated and stealthy attacks are detected as they happen. It improves effectiveness against file-less technique by hunting for and identifying hard-to-detect, sophisticated, cutting-edge attacks and generating meaningful alerting and precise guided remediation advice.

Security professionals need to account for the existence of fileless malware and fileless attacks in their security strategies.

Vulnerability Watch

Critical Vulnerability in Red Hat OpenStack Platform

Source: cisco.com

RED HAT® OPENSTACK® PLATFORM

Vulnerability in Red Hat OpenStack could allow an unauthenticated, remote attacker to gain unauthorized access to a targeted system. The vulnerability is due to improper authentication and encryption standards that are set by default when the *libvirtd* component is deployed by the affected software.

A successful exploit could allow the attacker to gain unauthorized access to the targeted system, which could allow the attacker to gain control of the host. Red Hat has confirmed the vulnerability and released software updates.

To exploit this vulnerability, the attacker may need access to network in which the targeted system resides. This access requirement could reduce the likelihood of a successful exploit. Administrators are advised to apply the appropriate updates, to allow only trusted users to have network access, to allow only privileged users to access administration or management systems and to monitor affected systems.

CVE ID: CVE-2017-2637.

Note: Organisations should implement controls like privilege segregation, timely and appropriate updates, Virus scan and active monitoring of network. Regular backup of critical data is the best practice for any post incident restoration activity and Business Continuity Plan.

Patch Samba to Address Wormable Code Execution Bug

Source: hipaajournal.com

A worldwide cyberattack similar to WannaCry could be repeated using Windows Server Message Block (SMB) vulnerability. US-CERT and NCIIPC had issued security alerts advising organizations to apply patch as soon as possible. The vulnerability, affects Samba 3.5.0 and later versions. Samba provides Windows style file and print services for Linux and UNIX servers and is based on the Windows SMB protocol. The flaw is a remote code execution vulnerability that could be exploited to upload a shared library to a writable share, and then cause the server to load and execute it. If the flaw is exploited, an attacker could run arbitrary code with root-level permissions. The flaw can only be exploited on un-patched computers if port 445 is open to the Internet and if a machine permits permanent write privileges from a shared file with a known or guessable server path. A patch has been issued to fix the vulnerability in Samba version 4.4 and later.

Samba is also used on NAS devices, often without user's knowledge. NAS environments are commonly used to store backup files. Organizations should therefore ensure that at least one copy of backup file is stored on an offline, non-networked device.

Organizations should therefore ensure that at least one copy of backup file is stored on an offline, non-networked device.

Security App

Wannakey

Source: github.com

This software allows recovering the prime numbers of RSA private key that are used by WannaCry. It does so by searching for them in the wcry.exe process. This is the process that generates the RSA private key. The basic principle is that the *CryptDestroyKey* and *CryptReleaseContext* do not erase the prime numbers from memory before freeing the associated memory. This is not really a mistake from the ransomware authors, as they properly use the Windows Crypto API. Under Windows 10, *CryptReleaseContext* does cleanup the memory (and so this recovery technique won't work). It can work under Windows XP because, in this version, *CryptReleaseContext* does not do the cleanup. If you are lucky (that is the associated memory hasn't been reallocated and erased), these prime numbers might still be in memory. That's what this software tries to achieve. If the key had been successfully generated, you will just need to use the "Decrypt" button of the malware to decrypt your files!

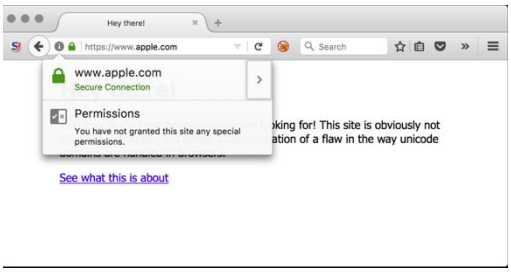
The basic principle is that the CryptDestroyKey and CryptReleaseContext do not erase the prime numbers from memory before freeing the associated memory.

Homographs

Source: isc.sans.edu

There is a campaign going on where phishing attacks use domains that look exactly like safe domains by using Punycode domains. This is called a homograph attack. The Punycode domains start with xn-- prefix and browsers will show the decoded Unicode domain name in the address bar where the Unicode characters (homographs) used appears like the original characters. This tool will generate a table of all homographs (identical characters) within a font and create a list of all possible domains. For Phishing campaigns not only homograph domains could be used, but also the glyphs with small changes. When using for example URL *https://www.xn--80ak6aa92e.com/*, you'll see (in Firefox and Chrome) in your address bar *https://www.apple.com/*. It is possible to request SSL certificates (using Let's Encrypt) with Punycode domain names, making this attack even more dangerous. The address bar will appear secure and contain the safe domain name making it impossible to recognize the difference.

Firefox, Chrome and Opera browsers are vulnerable to the homograph attack, whereas the Chrome will fix this issue. Within Firefox the support for Punycode can be disabled by navigating to about:config and disabling "network.IDN_show_punycode".



URL https://www.xn--80ak6aa92e.com/ being shown as https://www.apple.com

Within Firefox the support for Punycode can be disabled by navigating to about:config and disabling "network.IDN_show_punycode".

NCIIPC Initiatives

Sensitization Program on Ransomware Attack for Delhi Government

Sectoral Coordinator, Government

Department of Information Technology, Government of NCT of Delhi in collaboration with NCIIPC organised sensitization program on recent Ransomware attack 'WannaCry' for the employees of the Delhi Government. Representatives from all the departments involved in e-governance and digital projects participated in the said program which was held at the Delhi Secretariat. Sectoral Coordinator (Government), NCIIPC delivered the sessions covering the advisories released by NCIIPC during the 'WannaCry' attack. Sessions also outlined the pro-active preventive measures in form of do's and don'ts to be adopted by employees for practicing safe hygiene practices as per Information Security policy of the organisation for circumventing these types of threats. Sh. Santulan Chaubey, Director-DeGS & CISO, Government of NCT of Delhi coordinated the event.

Sh. Navdeep Pal Singh, Sectoral Coordinator (Government)

Workshop on Cyber Security for Power Infrastructure in India

Sectoral Coordinator, Power & Energy

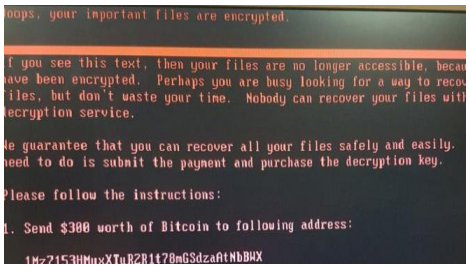
The Independent Power Producers Association of India (IPPAI) successfully conducted a workshop to create awareness and to provide training to implement cyber security for power infrastructure, under the aegis of the Central Electricity Authority (CEA) and NCIIPC, at the Southern Regional Power Committee (SRPC) Conference hall, Bengaluru on 8 June 2017. This initiative taken by NCIIPC seeks to increase preparedness among key power system constituents in each region of the country. The Central Electricity Authority has invited 33 key constituents: electricity distribution companies, transmission companies and power producers for the workshop. This workshop has covered various topics concerned to the cyber security of critical infrastructure.

The Central Electricity Authority has invited 33 key constituents: electricity distribution companies, transmission companies and power producers for the workshop.

Blocking of Phishing Websites

Sectoral Coordinator, BFSI

Recently it was observed that phishing websites are posing significant risks to Critical Information Infrastructure (CII) of BFSI sector. The phishing websites of certain banks were reported on 23rd and 24th March 2017 respectively. NCIIPC reported these sites to the concerned registrars and wrote to the concerned DNS/Hosting Service Providers to suspend/block their Domain Name Services (DNS).



The ransomware displays a text, demanding $300 worth of bitcoin

Petya ransomware replaces the computer's MBR with its own malicious code that displays the ransom note and leaves computers unable to boot.

Create a file i.e. "C:\Windows\perfc" to prevent ransomware infection.

NCIIPC advisory on PetrWrap ransomware

Source: nciipc.gov.in

A new variant of Petya ransomware, also known as Petrwrap, is spreading rapidly using the Windows SMBv1 vulnerability**.** Petya is a nasty piece of ransomware and works very differently from other ransomware. Unlike other traditional ransomware, Petya does not encrypt files on a targeted system one by one. Instead, Petya reboots victim's computer and encrypts the hard drive's Master File Table (MFT) and renders the Master Boot Record (MBR) inoperable, restricting access to the full system by seizing information about file names, sizes, and location on the physical disk. Petya ransomware replaces the computer's MBR with its own malicious code that displays the ransom note and leaves computers unable to boot. Petya ransomware has infected IT systems in various countries:

- Russia: State-owned oil giant Rosneft.
- Ukraine: Ukrainian state electricity suppliers: Kyivenergo and Ukrenergo, National Bank of Ukraine (NBU) and Oschadbank, Ukrainian telecommunication operators: Kyivstar, LifeCell, Ukrtelecom.
- US: Pharma Giant Merck.
- UK: Britain's WPP, the world's biggest advertising agency.
- IT systems of shipping giant A.P. Moller-Maersk impacted at multiple locations and business units.

PT Security, a UK-based cyber security company and Amit Serper from Cybereason, have discovered a Kill-Switch for Petya ransomware. According to a tweet, company has advised users to create a file i.e. "C:\Windows\perfc" to prevent ransomware infection.

Upcoming Events

July 2017

- Black Hat USA 2017, Las Vegas — 22-27 Jul
- IEEE International Conference on Smart Grid and Smart Cities, Singapore — 23-26 Jul
- RSA Conference 2017, Singapore — 26-28 Jul
- DEF CON 25, Las Vegas — 27-30 Jul
- International Conference on Networks and Security, Chennai — 29-30 Jul

August 2017

- Indianapolis Tech Security Conference — 3 Aug
- CLOUDSEC Hong Kong 2017 — 3 Aug
- International Conference on Cyber Security, Kota — 12-13 Aug
- International Workshop on Networks and Information Security, Taichung — 13-16 Aug
- Usenix Security Symposium, Canada — 16-18 Aug
- c0c0n 2017, Kochi — 18-19 Aug
- FINTECH Security Summit 2017, Singapore — 25 Aug
- CyberCon Asia 2017, Philippines — 25-26 Aug
- Fifth International Conference of Security, Privacy and Trust Management, Dubai — 26-27 Aug
- Gartner Security & Risk Management Summit 2017, Mumbai — 29-30 Aug

September 2017

- Security Bsides, Amsterdam — 1 Sep
- ENIGMA 2017, Pune — 2 Sep
- Incident Response 2017, Pentagon City — 11-12 Sep
- HP Protect 2017, Washington — 11-13 Sep
- OWASP AppSec USA 2017, Orlando — 19-22 Sep
- International Conference on Cyber-Security in Aviation, Computer Science and Electrical Engineering, Grand Forks — 21-23 Sep

JULY 2017

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

AUGUST 2017

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

SEPTEMBER 2017

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

SEPTEMBER 2017

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

OCTOBER 2017

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				

- National Information Security Summit, Lucknow 24 Sep
- IEEE Secure Development Conference, Cambridge 24-26 Sep
- The Cyber Security for Critical Infrastructure, Houston 27-29 Sep

October 2017

- Virus Bulletin International Conference, Madrid 4-6 Oct
- (ISC)2 Secure Johannesburg 2017 5 Oct
- BruCON, Belgium 5-6 Oct
- EC-Council Global CISO Forum 2017, Atlanta 9-10 Oct
- ISSA International Conference, San Diego 9-11 Oct
- Cloud and Cyber Security Expo, Singapore 11-12 Oct
- InfoSec Intelligence Conclave 2017, Bangalore 12-13 Oct
- ISACA Ireland Conference 2017 20 Oct

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.