THE CYBER TIME

An initiative towards cyber security....

I am glad to know that the students of M.S. Cyber security are bringing out this newsletter every month. As all are aware, this is cyber world and Govt. of India has also formulated a policy for prevention of cybercrime and related issues. I wish, this newsletter will play a key role in creating awareness among students and society towards cyber security and related domain.

Sh. M.L. Nehra (R.A.S)
Registrar
SPUP, Jodhpur

ACKNOWLEDGEMENT

We are very thankful to college administration as well as Department of cyber security for supporting us. We are also thankful to Mr. Arjun Chaudhary & Mr. Vikas Sihag for providing us quizzes and other guidance.

Edition Highlights

- ✓ *Free Wi-Fi*
- ✓ *Back off, virus targeting credit card data prowls in Cyberspace*
- ✓ *VIRUS TO WINDOWS OS - BLADABINDI*
- ✓ *List of data breaches and cyber-attacks in August*
- ✓ *IT ACT Beware of being Criminal*
- ✓ *Quiz*
- ✓ *Crossword*

Free Wi-Fi

-Nishant Grover

In real world, a piece of cheese is used to lurk mouse to trap and thus this greed takes his life. The digital world is more dangerous, although it will not harm you physically but it can rob your personal data from the air you are breathing while you are busy checking your emails and messages. Most of the people when see an icon of free/open Wi-Fi on laptop and smartphones, tend to connect it and surf internet and when they does, the data from devices travel through air without any security of encryption, that means it is readable to anyone who can read the packet. Normally, only the gateway (modem) read your packet, but what if someone else is also hearing? In less than 5 minutes, you can lose your social networking identity, in 10 minutes you might lose your banking account details, worse will happen when same password is used for multiple accounts.

There are 3 ways a hacker exploits public Wi-Fi hotspot. The first method is **Man in the middle attack**, hacker injects himself between two computers. Let's say your computer and a shopping website on which you are placing your order. He can intercept and modify the communication packets, and thus can acquire your banking details or personal details.

Second method is through **Rogue Wi-Fi network**. A hacker sets up fake networks that masquerade as legitimate networks to steal information from unsuspecting users who connect to it. This can easily be done through a laptop or a mobile device. The third method is **Packet sniffing**. A hacker downloads ready to use software which allows him to intercept any information sent over unsecured Wi-Fi. **Every year 6 Billion accounts details are leaked globally, only 5% of internet users are aware of risks of public Wi-Fi.**

There are number of methods a user can deploy to protect its data even in open Wi-Fi hotspots. The first and easiest method is not to favor open Wi-Fi over secured home and office network. If you see multiple Wi-Fi with similar name, do confirm the actual Wi-Fi network name with business owner. Also, deploy anti-virus and firewall to prevent unauthorized access to your machine preventing anyone accessing your hard disk. Many websites provide two factor authentication for accounts, so even if your login credentials are leaked, hacker still won't be able to access account. When visiting websites, only visit those who provide https protocol, https allow you to encrypt data when it is being transferred from your browser thus making it unreadable for any party sitting in middle. Other way to encrypt your data is using VPN, Virtual Private Network allows you to encrypt your data, and it also hides your address and provides you a new IP address. If you use public Wi-Fi connections regularly, you may want to invest in a VPN. As a bonus, a VPN will allow you to bypass any filtering and website-blocking in place of the public Wi-Fi network, allowing you to browse whatever you want. Do note, secured Wi-Fi (the one with passwords) provide built in encryption of data, so feel free to connect to them if you know the password.

India's top 8 cities will soon be availing free Wi-Fi hotspots at public places, with unaware public, the amount of information leaked to dark world of internet will be unthinkable. Hopefully readers of this article will think twice before connecting to unsecure Wi-Fi hotspots until then stay secure, stay protected and don't be a mouse!

Q.1.Which industry suffers the most data breaches?

A. Health care
B. Financial
C. Retail
D. Restaurant

Backoff, virus targeting credit card data prowls in Cyberspace

- Karma Ram

Vinod Parihar

This advisory was prepared in collaboration with the National Cyber security and Communications Integration Center (NCCIC), United States Secret Service (USSS), Financial Sector Information Sharing and Analysis Center (FS-ISAC), and Trust wave Spider labs, a trusted partner under contract with the USSS. The purpose of this release is to provide relevant and actionable technical indicators for network defense against the PoS malware dubbed "Backoff" which has been discovered exploiting businesses' administrator accounts remotely and exfiltration consumer payment data.

The virus, of the lethal 'Trojan' family, has been named "Backoff" and is being seen spreading through computer networks which use Windows as their operating systems.
"It has been reported that variants of malware family dubbed as 'Backoff' targeting Point of Sale (POS) systems are spreading. The malware mainly infects windows based systems. The malware propagates by scanning for systems with remote desktop applications enabled.

"Successful compromise allows an attacker to infect the systems further with the POS malware so as to steal customer payment cards data like card holders name, account number, expiration data, CVV code among others from POS systems," the CERT-In said in its latest advisory to Internet users in the country.

The CERT-In is the nodal agency to combat hacking, phishing and to fortify security-related defenses of the Indian Internet domain.
The virus is so notorious that it is able to capture keystrokes and communicate with the command and control server for further hacking-like activity, the agency warned.
Interestingly, the virus also possesses capability to inject malicious stub into Windows 'Explorer.exe' for persistence and in case the malicious file crashes or is stopped forcefully, the agency said.
Cyber security sleuths said the malware and all its variants remain "mostly undetected by the anti-virus vendors" which categorizes it as a potent and big threat in the online world.

"The malware makes a network connection to various command and control servers and uses HTTP POST request to transfer the data of the victim system. The POST requests generated from the victim machine consist of various parameters identifying different information about the infected machine," the advisory said about the virus which can acquire at least three aliases to hide its evil designs.
The agency has suggested some countermeasures in this regard.

"Keep all POS systems thoroughly updated including POS application software, do not allow administrative access to systems, delete the system changes made by the malware such as files created or registry entries or services among others, limit or eliminate use of shared or group accounts, disable auto run or auto play.

"Do not visit untrusted websites, enable firewall at gateway or desktop level, do not download or open attachment in emails received from untrusted sources or unexpectedly received from trusted users and install and scan anti-malware engines and keep them up-to-date," the agency recommended.

Description

"Backoff" is a family of PoS malware and has been discovered recently. The malware family has been witnessed on at least three separate forensic investigations. Researchers have identified three primary variants to the "Backoff" malware including 1.4, 1.55 ("Backoff", "goo", "MAY", "net"), and 1.56 ("LAST").These variations have been seen as far back as October 2013 and continue to operate as of July 2014. In total, the malware typically consists of the following four capabilities. An exception is the earliest witnessed variant (1.4) which does not include key logging functionality. Additionally, 1.55 'net' removed the explorer.exe injection component:

- Scraping memory for track data
- Logging keystrokes
- Command & control (C2) communication
- Injecting malicious stub into explorer.exe

The malicious stub that is injected into explorer.exe is responsible for persistence in the event the malicious executable crashes or is forcefully stopped. The malware is responsible for scraping memory from running processes on the victim machine and searching for track data. Key logging functionality is also present in most recent variants of "Backoff". Additionally, the malware has a C2 component that is responsible for uploading discovered data, updating the malware, downloading/executing further malware, and uninstalling the malware.

Q.2. How many credit card numbers were stolen in the largest known cyber theft?

A. 10 million
B. 90 million
C. 130 million (heartland reach)
D. 215 million

The way to build a nation is to build a good citizen. The majority of the citizens should be efficient, of good character and possess a reasonable high sense of duty.

-Mokshagundam Visvesvarayya

VIRUS TO WINDOWS OS - BLADABINDI

- Pragya Johari

Is your device running on Microsoft Windows OS? You might have faced few situations like your personal or crucial information has been hacked by someone else. It is proved that your PC/Laptop has been attacked by a dangerous program called **"Bladabindi Virus".**

Introduction:-

The Bladabindi malware family can steal your sensitive information and send it to a malicious hacker. They can also download other malware and give backdoor access to your PC. They can spread via infected removable drives, like USB flash drives. They can also be downloaded by other malware, or spread though malicious links and hacked websites.

This Multi-identity virus "Bladabindi" steals sensitive personal information of a user for nefarious purposes. This virus is a backdoor type that means this can bypass normal authentication, obtaining access to plaintext, while attempting to remain undetected.

This malware steals sensitive information from infected computer system. This could also be used as malware downloader and provide backdoor access to the remote attacker. This virus is infecting specially Microsoft Windows Operating System. Some of the Bladabindi variants could capture keyboard press, control computer camera and later send collected sensitive information to remote attacker. If your PC is lay into Bladabindi then this nasty virus could corrupt all your files, creates shortcut file, copying into root folder, etc. This potential infecting program could endeavors to access all the personal data that leads to damage or loss of significant proprietary information of a user such as:

- Computer name
- Computer's OS (Operating System) version
- Country and serial number
- Windows user name
- #Chrome stored passwords
- #Firefox stored passwords

CERT-In has said that Bladabindi virus can use up to 12 false identities to mask its real identity and it can be easily created through a malicious hacker tool which is available publicly.

Aliases:-Trojan.MSIL.Disfa.bsto (Kaspersky), winpe/Troj_Generic.OEKLP (Norman), Generic34.AXLL (AVG), TR/MSILKrypt.6.258 (avira), Gen:Variant.MSILKrypt.6 (BitDefender), Win32.HLLW.Autoruner.25074 (Dr.Web), MSIL/Injector.BOX Trojan (ESET), MSIL/Injector.PEW!tr (Fortinet), TR/Bladabindi.J.1 (Avira), Trojan.Bladabindi!4BAD (Rising AV), Troj/Bbindi-A (Sophos), Trojan/Win32.Jorik (AhnLab), W32/Bladabindi.D (Norman), Trojan.Bladabindi!4D1D (Rising AV).

A typical 'Bladabindi' variant propagates by way of copying themselves into the root folder of a removable drive and create a shortcut file with the name and folder icon of the drive. When the user clicks on the shortcut, the malware gets executed and Windows Explorer is opened and it makes it seem as if nothing malicious happened. "The malware can also use infected computer's camera to record and steal personal information. It checks for camera drivers and installs a DLL plugin so it can record and upload the video to a remote attacker. The malware can also log or capture keystrokes to steal credentials like user names and passwords,"

Backdoor: Bladabindi variants copies itself to the following locations:
It copies itself to the startup folder to make sure it runs each time system boot up.
<startup folder>\<32 random alpha- numeric characters>.exe

For example <startup folder>\5cd8f17f4086744065eb0992a09e05a2.exe

- %TEMP% \<variable name>.exe
- for example %TEMP%\svhost.exe
- %APPDATA%
- %USERPROFILE%
- %windir%

Precautions against Malicious Bladabindi Virus:-

- Scan your PC/desktop system with free anti-virus removal tools.
- Disable Autorun functionality.
- Must use "USB vaccination" and "USB clean" software.
- Keep latest and up-to-date application software.
- Fixes and patches of your OS.
- Ensure to have upgraded anti-spyware, anti-virus.
- Do not visit un-trusted websites.
- Generate strong passwords and also enable password policies too.
- Enable firewall at desktop and limited user rights.

Reference:-

http://www.cert-in.org.in

Q.3. Are you allowed to store personal information on a mobile device?

A. No, never
B. Yes, provided the information is limited to names and personal contact information
C. Yes, provided the device is password protected
D. Yes, provided the device is encrypted

List of data breaches and cyber-attacks in August

-Sumeet Mangal

Below is the list of Cyber-attacks and data Breaches took place in August, 2014. It doesn't surprise me that it's getting worse each month, though: after all, cyber threats are always increasing. Be sure to share this list with your friends and colleagues. Cyber threats will only decrease once the majority of people are aware of how serious they are and start taking action.

Data Breaches

- Records of 25,000 Homeland Security Employees Stolen in Cyber Attack
- Over 50 UPS franchises hit by data breach
- 4.5 Million Records Stolen from US Health Giant
- Supervalu supermarket chain investigating Albertson's stores hacked for credit card data breach
- Goodwill and FBI Investigate Possible Security Breach
- Kim and his 2 billion won: Massive data breach affects half of South Korean citizens
- Russian hackers steal 4.5 billion records
- Hackers Steal Passwords of Meet Me Social Network Users
- Chinese Hackers Allegedly Steal 4.5 Million Patient Records
- Jersey City Medical Center reports Medicaid patient breach
- Florida bank notifies roughly 72,500 customers of breach
- Insider breach at Las Vegas brain and spine surgery center
- Los Angeles-based health system breached; more than 500 patients affected
- Subcontractor breach impacts more than 60K Tennessee workers
- East Midlands Ambulance Service patient records disk 'missing'

Payment Information

- POS malware infections at two OTTO pizzeria locations in Maine
- Payment cards used on Wireless Emporium website compromised by malware
- Albertson's stores hacked for credit card data
- Black Market Cannabis Road Hacked, $100,000 in Bit coin Lost
- FBI Probes Possible Hacking Incident at J.P. Morgan

Social Media

- Microsoft and Sony's Twitch Accounts Were Hacked And Vandalized
- Russian PM's Twitter hacked, posting 'I resign'

DDoS

- Massive 300Gbps DDoS attack on media firm fuelled by unpatched server flaw
- Twitch hit with DDOS attack
- Sony suffer DDoS attack and threat forces executives' flight to make unscheduled landing
- Teenager hacked into Metropolitan Police's computer – causing force's website to crash

Other

- Saudi TV website hacked by Libyan
- Norwegian oil industry under attack by hackers
- Android apps riddled with security vulnerabilities
- US Cyber Crime Goes Nuclear: NRC Computers Hacked THREE Times
- Ferguson police officers computers hacked, FBI investigating.

Disclaimer: - This is not purely my work, thanks for other web pages for helping providing these information's on regular basis.

Personality Profile Dr. C. R. Rao

Calyampudi Radhakrishna Rao, FRS known as C R Rao (born 10 September 1920) is an Indian-born, naturalized American, mathematician and statistician. He is currently professor emeritus at Penn State University and Research Professor at the University at Buffalo. Rao has been honored by numerous colloquia, honorary degrees, and festschrifts and was awarded the US National Medal of Science in 2002.The American Statistical Association has described him as "a living legend whose work has influenced not just statistics, but has had far reaching implications for fields as varied as economics, genetics, anthropology, geology, national planning, demography, biometry, and medicine." The Times of India listed Rao as one of the top 10 Indian scientists of all time.

Academic Carrier

- M.A. (Mathematics):- Andhra University (1940)
- M.A. (Statistical):- Calcutta University (1943)
- Joined ISI (Indian statistical Institute) in 1943 as a Technical worker.
- He was deputed to work at the Museum of Archeology and Ethnology at Cambridge University in 1946.
- PhD: - Kings College in Cambridge University (1948)
- ScD: - Cambridge University (1965)

He was also awarded 36 Doctorate degrees from Universities in 19 countries spanning 6 continents. He is a member of eight National Academies in India, the United Kingdom, the United States, and Italy.

Academic and Research achievements

Rao is one of the pioneers who developed statistics from ad hoc origins into a firmly grounded Mathematical science. Among his best-known discoveries are the Cramer–Rao bound and the Rao–Blackwell theorem, Rao's Score test, Fisher-Rao metric, Rao distance, Rao measure, Cramer-Rao functional, Neyman-Rao test, Fisher-Rao theorem, Rao's theorem on second order efficiency, Rao's U test, Rao-Yanoi generalized inverse, Lau-Rao, Kagan-Linnik-Rao and lau-Rao Shanbag theorems. Other areas he worked in include multivariate analysis, estimation theory, and differential geometry. His other contributions include the Fisher–Rao Theorem, Rao distance, and orthogonal arrays. He is the author of 14 books and has published over 400 journal publications.

Awards and honors

- Calcutta University Gold medal (1943)
- SS Bhatnagar Award (1963)
- Guy silver medal by Royal statistical society (1965)
- Megnad Saha medal by INSA (1969)
- JC Bose Gold medal (1979)
- Wilks memorial Medal by American Statistical Association (1989)
- Mahalanobis Birth centenary Medal (1996)
- Padma Vibhushan (2001)
- Mahalanobis lifetime achievement award (2003)
- Srinivasa Ramanujan medal by INSA (2003)
- The national medal of science, USA India science award (2009)
- Guy Medalin Gold of Royal Statistical society (2012)

He was also elected fellow of the Royal Society, UK (1967), National Academy of Sciences, USA (1995), the academy of Sciences for the Developing world (1983) Lithuanian Academy of Sciences (1997), and Honorary Fellow of numerous International societies. He is also honored with the institutions of a prize in his name by the Govt. of India and there is also an institute by his name in the campus of the University of Hyderabad.

References

- www.insaindia.org
- www.wikipedia.org

Compiled By: Nitish Vyas

Q.4.Which of the following refers to the transforming of data into an unreadable format, so as to hide it from unauthorized individuals?

A. HTTP
B. Encryption
C. Digital Certificate
D. Phishing

Previous Quiz winner-

IT ACT Beware of being Criminal

-Hetram Yadav

Sec43: If any person without permission of the owner accesses computer or computer system, computer resource or computer network or copies, downloads, delete, modify data from an unauthorized system. If he/she become cause of denial of service for the legitimate user will be punishable under this section.

43-A- if an organization dealing with the sensitive data is negligent in implementing reasonable security measures, such a corporation will be liable to pay damage.

Punishment: Punishable according to section 66 with imprisonment up to 3 years or fine up to 5 lakh rupees or both.

Sec 65: For tempering the computer source code

Punishment: imprisonment up to 3 years or fine up to 2 lac rupees or both

Sec 66:

66-A - If anyone person sends an offensive or deceiving message by means of electronic device like computer or mobile

Punishment: imprisonment up to 3 years with fine

66-B: For receiving stolen computer or any electronic device

Punishment: imprisonment up to 3 years with fine of 1 lakh rupees

66-C: Punishment for ID, electronic signature or password theft

Punishment: imprisonment up to 3 years with fine of 1 lakh rupees

66-D: Cheating someone by using computer resource

Punishment: imprisonment up to 3 years with fine of 1 lakh rupees

66-E: If someone captures or transmits images of private area of a person without his/her concern

Punishment: Imprisonment up to 3 years with fine of 2 lakh rupees

66-F: Punishment for cyber terrorism (affecting integrity, security, unity of India)

Punishment: Lifetime imprisonment

67: Punishment for publishing or transmitting obscene material in electronic form

67A: Transmitting a material containing sexually explicit act in electronic form

Punishment: Five years of imprisonment with rupees ten lakhs fine

67B: Publishing or transmitting of material depicting children in sexually explicit act

Punishment: Five years of imprisonment with rupees ten lakhs fine

Departmental News:

1) **CBI** signs a Memorandum of Understanding **(MoU)** With Sardar Patel University of Police, Security & Criminal Justice (SPUP), Jodhpur to Enhance the Quality of Investigation and Prosecution of Crime.

2) Visit of Dr. **Ponnurangam Kumaraguru** (Assistant Professor **IIIT- Delhi**)

3) Introducing **"AndroClub"** for android develop and analysis application.

4) Teachers Day Celebration.

Picture Credit- Arjun Suthar

Q.5. When a user needs to provide message integrity, what options may be best?

A. Send a digital signature of the message to the recipient
B. Encrypt the message with a symmetric algorithm and send it
C. Encrypt the message with a private key so the recipient can decrypt with the corresponding public key
D. Create a checksum, append it to the message, encrypt the message, and then send to recipient.

CyberSec Puzzle

Across

3. Reassigned value or setting that is used by the computer when a value or setting is not specified by the program user.

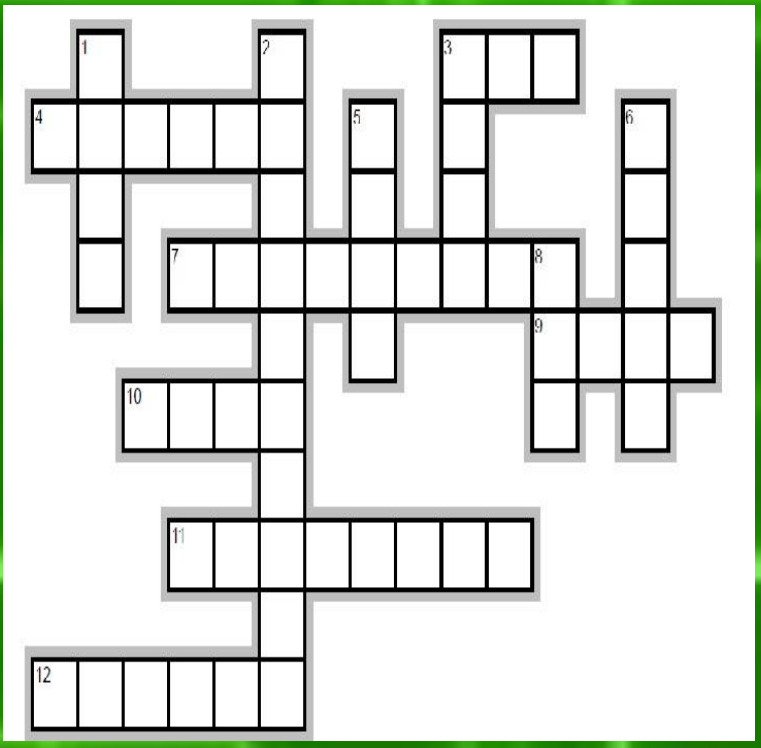
4. It is popular web search engine developed by two graduate student who met at Stanford University.

7. Temporary storage area for data that a user wants to copy one place to another.

9. It is a term for spam messages sent to instant message addresses

10. A set of options presented to a user to help him or her find information or execute a program function.

11. A collection of information that is organized so that it can easily be accessed, managed, and updated.



Previous Crossword Answer

Across

2. Hacker

4. Blog

7. Trojan horse

9. Popup

10. Download

Down

1. Cyberbully

3. Adware

5. Worm

6. Password

8. Email

Down

1. It is often an email that mailed in chain letter fashion describing some devastating, highly unlikely type of virus.

2. It is etiquette on the internet.

3. It is the information that is stored and manipulated by programs.

5. It is an online abbreviation for 'You got to be kidding'.

6. Never forward this type of letters.

8. An abbreviation that means of accessing the internet at high speed using a standard phone line.

Contributed By: Yogendra Singh Chahar

Call for articles:

Students are invited to get involved in the TechNewsletter activities by providing articles and other related materials. Suggestions and feedbacks for the improvement of the newsletter are most welcome and contributions are invited from the faculty and students of the department. Contributions can be from any of the whole gamut of activities in the department like any special achievement, an admirable project, a publication, and Cyber Crime case, Quiz, puzzles or even the fun section material like jokes, cartoons, interesting facts or poems. You can also report any interesting workshops or talks taking place in the department.

You can send your material on: - **editors@policeuniversity.ac.in** by October 5, 2014.

Previous Quiz Answer

QUIZ: 2 https://www.facebook.com/help/delete_account

And after that 14 days are given. After 14 days, account will be deleted permanently.

Quiz 3 C. wreck Iranian nuclear centrifuges

Quiz 4 A. Hunt for Red October

Quiz 5 B. "Everyone can have their own cyber weapon."

Editorial Board:

Hetram Yadav

Nitish Vyas

Vikas Yadav

Pragya Johari

Please send the answers of quiz and crossword on editors@policeuniversity.ac.in till September 30, 2014. The winner will be declared on the basis of first come first serve with right answers. The name of the winners and answers will be published in the next edition.

Note: - If any of the article is found to be copied, the writer himself/herself will be responsible for copyright issues. Editor or University will not be liable for any such issues.

Brought out by the Department of Computer Science & Cyber Security
Sardar Patel University of Police, Security & Criminal Justice, Jodhpur