Information Security Education & Awareness
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India

InfoSec Newsletter

JAN–FEB 2016

सी डैक
CDAC

InfoSec Concept 4

CYBER ETHICS

For Virus Alerts,Incident & Vulnerability Reporting

cert-in

Handling Computer Security Incidents

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India

Nalanda Building, No. 1 Shivabagh Satyam Theatre Road,
Ameerpet, Hyderabad - 500016, Telangana (India)

Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway,
Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 500005, Telangana(India)

E-mail : isea@cdac.in

InfoSec

Newsletter
Jan - Feb 2016

Credits

Prof. N Balakrishnan
(IISc, Bangalore)
Prof. Sukumar Nandi
(IIT, Guwahati)
Prof. V Kamakoti (IIT, Madras)
Prof. M S Gaur (SVNIT, Jaipur)

Design & Technical Team
Ch A S Murty
I L Narasimha Rao
K Indra Veni
K Indra Keerthi
P.S.S.Bharadwaj

Action Group Members
HOD (HRD), DeitY
Shri.Sitaram Chamarthy (TCS)
Prof. M S Gaur (MNIT, Jaipur)
Prof. Dr.Dhiren R Patel
(NIT Surat)
Representative of Chairman
(CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasar Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, DietY

Compiled by
G V Raghunadhan
I L Narasimha Rao

From C-DAC
E Magesh, Director

Acknowledgement
HRD Division
Department of Electronics &
Information Technology
Ministry of Communications &
Information Technology
&
For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

InfoSec Quiz

1. An unauthorized person who secretly gains access to computer files?
   A) Hacker B) Bully

2. Malicious software that enters a computer and tracks and gathers personal information?
   A) Malware B) Virus

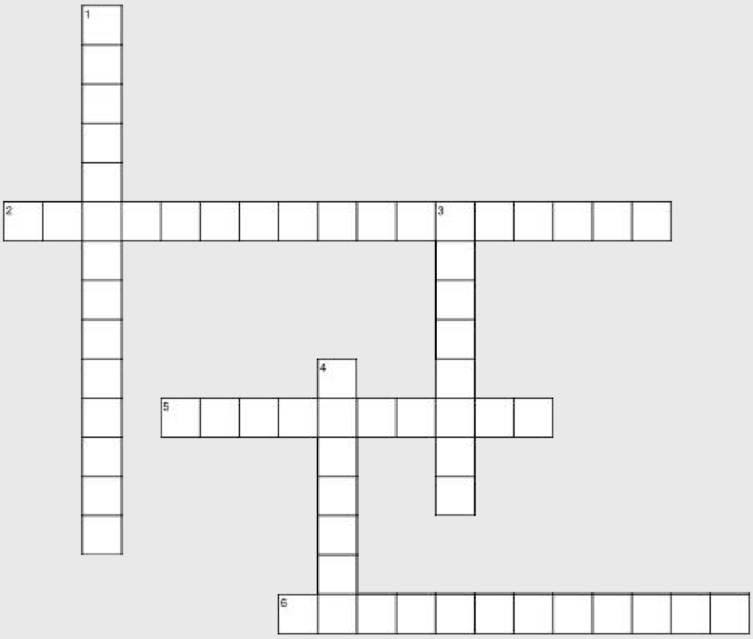
3. Tricking users into revealing personal information such as passwords and bank account numbers by way of emails pretending to be from actual companies?
   A) Phishing B) Spoofing

4. Using someone else's work and taking credit for it?
   A) Plagiarism B) Social engineering

5. A program that looks harmless, but has harmful code inside. When that software is activated it causes damage to your computer?
   A) Trojan Horse B) Worm

logon to
www.infosecawareness.in/contest
to participate in Infosec Contest and **WIN PRIZES**

InfoSec Crossword



Across

2 That exploits children for sexual stimulation
5 Public records search engines & databases are the main culprits contributing to the rise of
6 Study pertaining to the computers, encompassing user behaviour and what computers.

Down

1 It is raising rapidly due to the availability of private information in the Internet
3 It is often a topic in ethical debate as some view it as inherently wrong
4 It can be decomposed to the limitation of others access to an individual

InfoSec Tip

Guess The Tip

which best suits the cartoon by logging in to

www.InfoSecawareness.in

InfoSec Tip
Use Internet ethically

- DON'T use copyrighted information as your own. The Internet has such a wealth of information that it can be tempting to copy and reuse information you find online. Presenting information from the Internet as your own work is not only dishonest, it could be illegal. If the material is copyrighted, then by law it belongs to someone else. If you use it without permission or appropriate attribution, you might be violating copyright laws.

- DO enjoy music, videos and games on the Internet. There are many websites where you can sample new music, watch movies and other videos, or play and learn about computer games.

- DO use the Internet to expand your social and business networks. Social and business networking sites can help you locate old friends and make new ones, create and maintain valuable professional contacts, and build your online reputation.

CYBER ETHICS

Cyber-ethics is the discipline of using appropriate and ethical behaviors pertaining to computers, Internet and acknowledging moral duties and obligations pertaining to online environments and digital media and how this affects individuals and society

COMPUTER ETHICS

Ethics are a set of moral principles that govern an individual or a group on what is acceptable behavior while using a computer. Computer ethics is a set of moral principles that govern the usage of computers.

One of the common issues of computer ethics is violation of copyright issues. Duplicating copyrighted content without the author's approval, accessing personal information of others are some of the examples that violate ethical principles.

INTERNET ETHICS

Internet ethics means acceptable behavior for using Internet.

We should be honest, respect the rights and property of others on the Internet.

Everyone has to accept that Internet is not a value free-zone.

It means World Wide Web is not a waste wild web it is a place where values are considered in the broadest sense so we must take care while shaping content and services and we should recognize that Internet is not apart from universal society but it is a primary component of it.

Sensitivity to National and Local cultures

It belongs to all and there is no barrier of national and local cultures. It cannot be subject to one set of values like the local TV channel; or the local newspaper .We have to accommodate multiplicity of usage.

ISEA,Supported by DeitY,Government of India

While using e-Mail and chatting

Internet must be used for communication with family and friends. Avoid chatting with strangers and forwarding emails from unknown people/strangers. And we must also teach children about risks involved in chatting and forwarding emails to strangers.

Pretending to be someone else

We must not use Internet to fool others by pretending to be someone else. Hiding our own identity to fool others in the Internet world is a crime and may also be arisk to others. It's our responsibility to teach children the same.

Avoid Bad language

We must not use rude or bad language while using e-Mail, chatting, blogging and social networking, we need to respect their views and should not criticize anyone on the Internet and the same should be taught to children.

Hide personal information

We should teach children not to give personal details like home address, phone numbers, interests, passwords. No photographs should be sent to strangers and they should be asked to hide their personal details from strangers because it might be misused and shared with others without their knowledge.

While Downloading

Internet is used to listen and learn about music, It is also used to watch videos and play games. We must not use it to download them or share copyrighted material. The same should be taught to children, and they must be aware of the importance of copyrights and issues of copyright.

Supervision

You should know what children are doing on the Internet and the sites they visit on the Internet and should check with whom they are communicating. Restrict them browsing inappropriate sites. Parental involvement is essential when a child is using the Internet in order to make him follow the rules.

Ensure that you have policies regarding the use of e-mail and the Internet

Never download files through CHAT sessions from unknown persons

Encourage children to use Internet

We must encourage children, students and others to gain the knowledge from the Internet and use it wisely. Internet is a great tool where we can gather information, which can be used for learning.

Access to Internet

The Internet is a time-efficient tool for everyone that enlarges the possibilities for curriculum growth. Learning depends on the ability to find relevant and reliable information quickly and easily, and to select, understand and assess that information. Searching for information on the Internet can help to develop these skills. Classroom exercises and take-home assessment tasks, where students are required to compare website content, are ideal for alerting students to the requirements of writing for different audiences, the purpose of particular content, identifying and judging accuracy and reliability. Since many sites adopt particular views about issues, the Internet is a useful tool for developing the skills of distinguishing fact from opinion and exploring subjectivity and objectivity.

Ethical rules for computer users

Some of the rules that individuals should follow while using a computer are listed below:

- Do not use computers to harm other users.
- Do not use computers to steal others information.
- Do not access files without the permission of the owner.
- Do not copy copyrighted software without the author's permission.
- Always respect copyright laws and policies.
- Respect the privacy of others, just as you expect the same from others.
- Do not use other user's computer resources without their permission.
- Use Internet ethically.
- Complain about illegal communication and activities, if found, to Internet Service Providers and local law enforcement authorities.
- Users are responsible for safeguarding their User Id and Passwords.
- They should not write them on paper or anywhere else for remembrance. Users should not intentionally use the computers to retrieve or modify the information of others, which may include password information, files, etc..

SECOND ANNUAL APPRAISAL WORKSHOP

Shri. E. Magesh, Director C-DAC welcoming Shri K. Shankar, IPS, Additional Commissioner of Police, Chennai

Shri. CHAS Murty, Principal Technical Officer C-DAC welcoming Shri K. Shankar, IPS, Additional Commissioner of Police, Chennai

Shri K. Shankar, IPS, Additional Commissioner of Police addressing the audience

Participants at the Workshop held at IITM Tech park, IIT Madras, Chennai

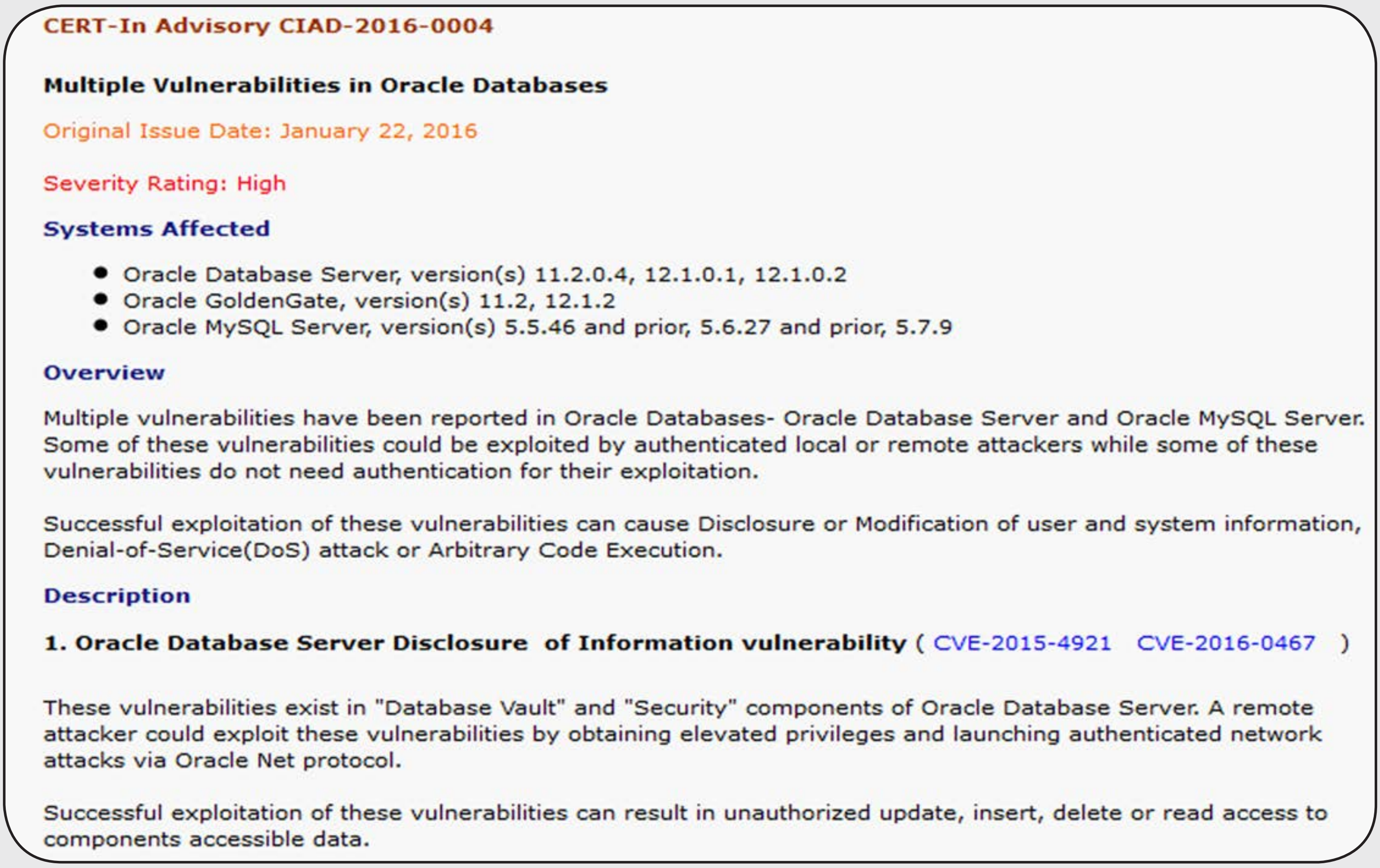
Shri Sanjay Kumar Vyas, Additional Director, DeitY addressing the audience

Launch of Cybercrime Awareness Posters

Launch of Cybercrime Awareness Stickers

Cybercrime Awareness Sticker being displayed at IITM ATM

ISEA,Supported by DeitY,Government of India



CERT-In Advisory CIAD-2016-0004

Multiple Vulnerabilities in Oracle Databases

Original Issue Date: January 22, 2016

Severity Rating: High

Systems Affected

- Oracle Database Server, version(s) 11.2.0.4, 12.1.0.1, 12.1.0.2
- Oracle GoldenGate, version(s) 11.2, 12.1.2
- Oracle MySQL Server, version(s) 5.5.46 and prior, 5.6.27 and prior, 5.7.9

Overview

Multiple vulnerabilities have been reported in Oracle Databases- Oracle Database Server and Oracle MySQL Server. Some of these vulnerabilities could be exploited by authenticated local or remote attackers while some of these vulnerabilities do not need authentication for their exploitation.

Successful exploitation of these vulnerabilities can cause Disclosure or Modification of user and system information, Denial-of-Service(DoS) attack or Arbitrary Code Execution.

Description

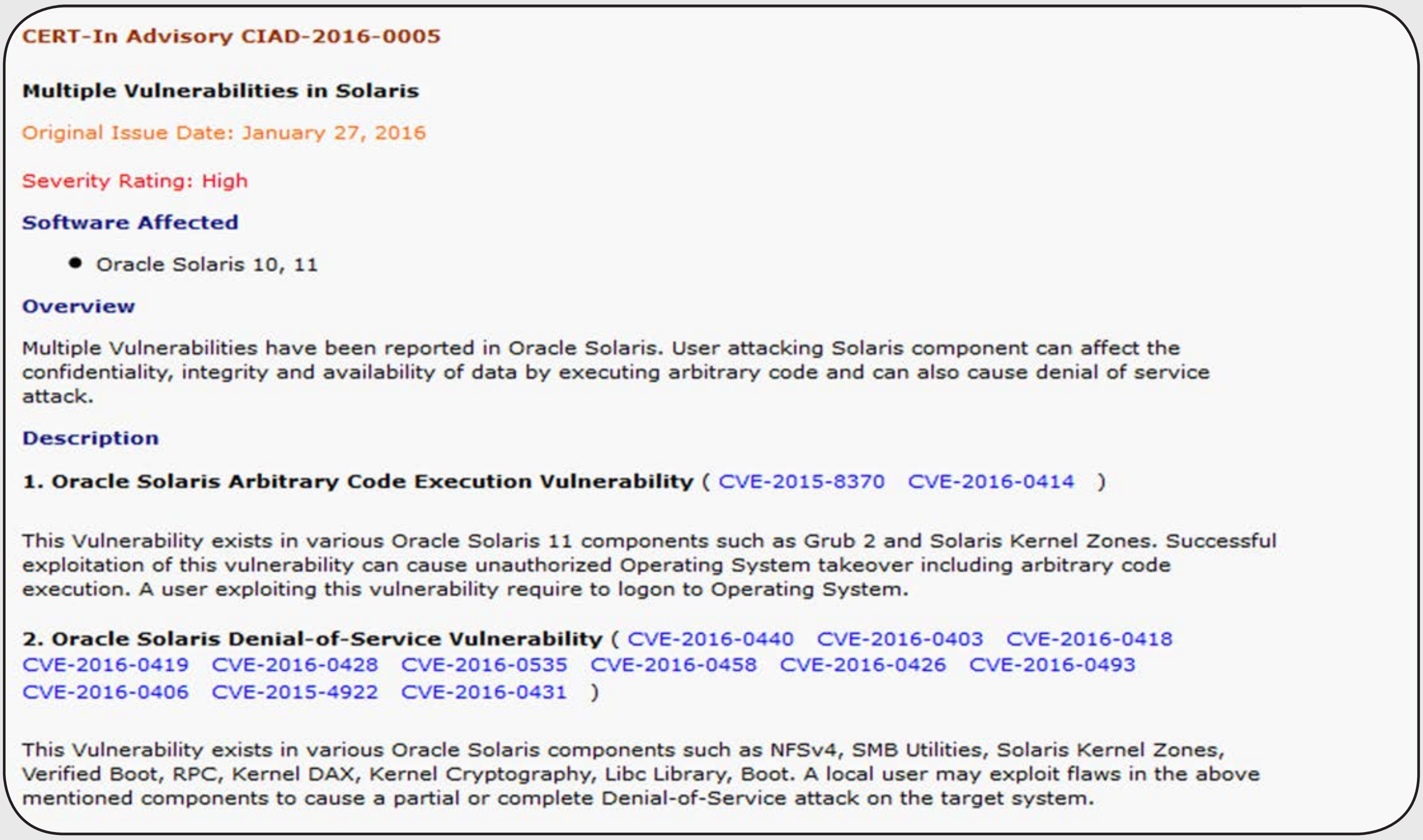
1. Oracle Database Server Disclosure of Information vulnerability (CVE-2015-4921 CVE-2016-0467)

These vulnerabilities exist in "Database Vault" and "Security" components of Oracle Database Server. A remote attacker could exploit these vulnerabilities by obtaining elevated privileges and launching authenticated network attacks via Oracle Net protocol.

Successful exploitation of these vulnerabilities can result in unauthorized update, insert, delete or read access to components accessible data.

For more details visit

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



CERT-In Advisory CIAD-2016-0005

Multiple Vulnerabilities in Solaris

Original Issue Date: January 27, 2016

Severity Rating: High

Software Affected

- Oracle Solaris 10, 11

Overview

Multiple Vulnerabilities have been reported in Oracle Solaris. User attacking Solaris component can affect the confidentiality, integrity and availability of data by executing arbitrary code and can also cause denial of service attack.

Description

1. Oracle Solaris Arbitrary Code Execution Vulnerability (CVE-2015-8370 CVE-2016-0414)

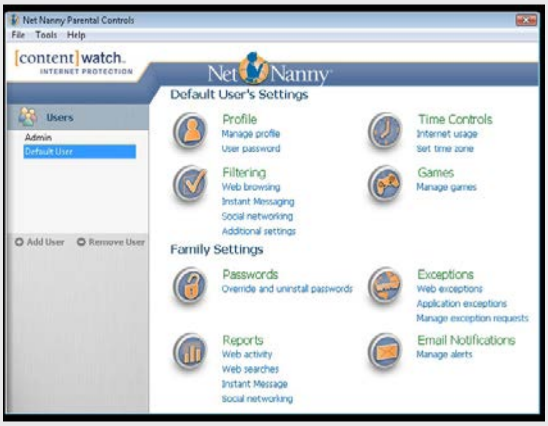
This Vulnerability exists in various Oracle Solaris 11 components such as Grub 2 and Solaris Kernel Zones. Successful exploitation of this vulnerability can cause unauthorized Operating System takeover including arbitrary code execution. A user exploiting this vulnerability require to logon to Operating System.

2. Oracle Solaris Denial-of-Service Vulnerability (CVE-2016-0440 CVE-2016-0403 CVE-2016-0418 CVE-2016-0419 CVE-2016-0428 CVE-2016-0535 CVE-2016-0458 CVE-2016-0426 CVE-2016-0493 CVE-2016-0406 CVE-2015-4922 CVE-2016-0431)

This Vulnerability exists in various Oracle Solaris components such as NFSv4, SMB Utilities, Solaris Kernel Zones, Verified Boot, RPC, Kernel DAX, Kernel Cryptography, Libc Library, Boot. A local user may exploit flaws in the above mentioned components to cause a partial or complete Denial-of-Service attack on the target system.

Net Nanny

Filtering & Blocking



This parental monitoring software can mask profanity, which is a huge bonus. You may want to allow your child to access sites like YouTube, for instance, but you don't want them to be bombarded by the colorful language in the comments. Net Nanny disguises that language with symbols instead. We love this product's tools for gaming too. You can block games based on their ESRB (Entertainment Software Rating Board) rating or specific content.

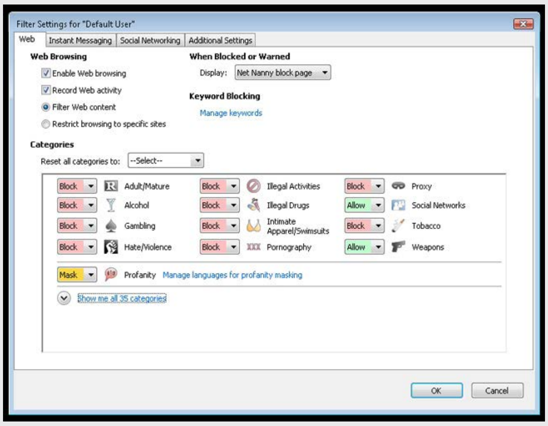
With Net Nanny, you get to control the quantity, not just the quality, of internet use for your children. School districts around the USA report that many children arrive at school sleep deprived. Tired children sometimes experience falling grades and can perform poorly on tests. Staying up late to play online games, chat with friends or simply surf the web, sometimes until the wee hours of the morning, have caused more than one child to experience sleep deprivation. Net Nanny comes equipped with a scheduling feature that can grant or deny children internet access. Parents can deny access during normal sleep hours.

Net Nanny's other filtering and blocking capabilities include website filtering, website blocking, and chat filtering and blocking. Recording Capabilities

Recording Capabilities

Net Nanny records all visited websites. Social networks pose numerous threats to children. Many parents have legitimate concerns regarding their child's online social networking profiles. Net Nanny may calm the fears of many parents because of its advanced social network monitoring capabilities. Parents can receive detailed reports regarding a child's Facebook, MySpace or other social networking profile. These detailed reports include a child's friends list, uploaded videos and pictures, wall posts and instant message conversations. To obtain this information, the monitored child must agree to install the targeted social network's app for Net Nanny on their personal profile. Should a child refuse permission, parents can easily block the child from accessing the site.

This parental software can capture transcripts of conversations that occur in chat and instant message applications. It even records Facebook and MySpace instant messaging. During the monitoring of internet-based conversations, the app proactively scans the exchanges for dangerous communications that may include the sexual solicitation of the child, bullying, threats, aggressive language and profanity. Upon identification of a potentially ominous word or phrase, the app alerts parents to the situation by email. It also records the words and keywords used to perform online searches.



Web Browsing

☑ Enable Web browsing

☑ Record Web activity

● Filter Web content

○ Restrict browsing to specific sites

When Blocked or Warned

Display: Net Nanny block page

Keyword Blocking

Manage keywords

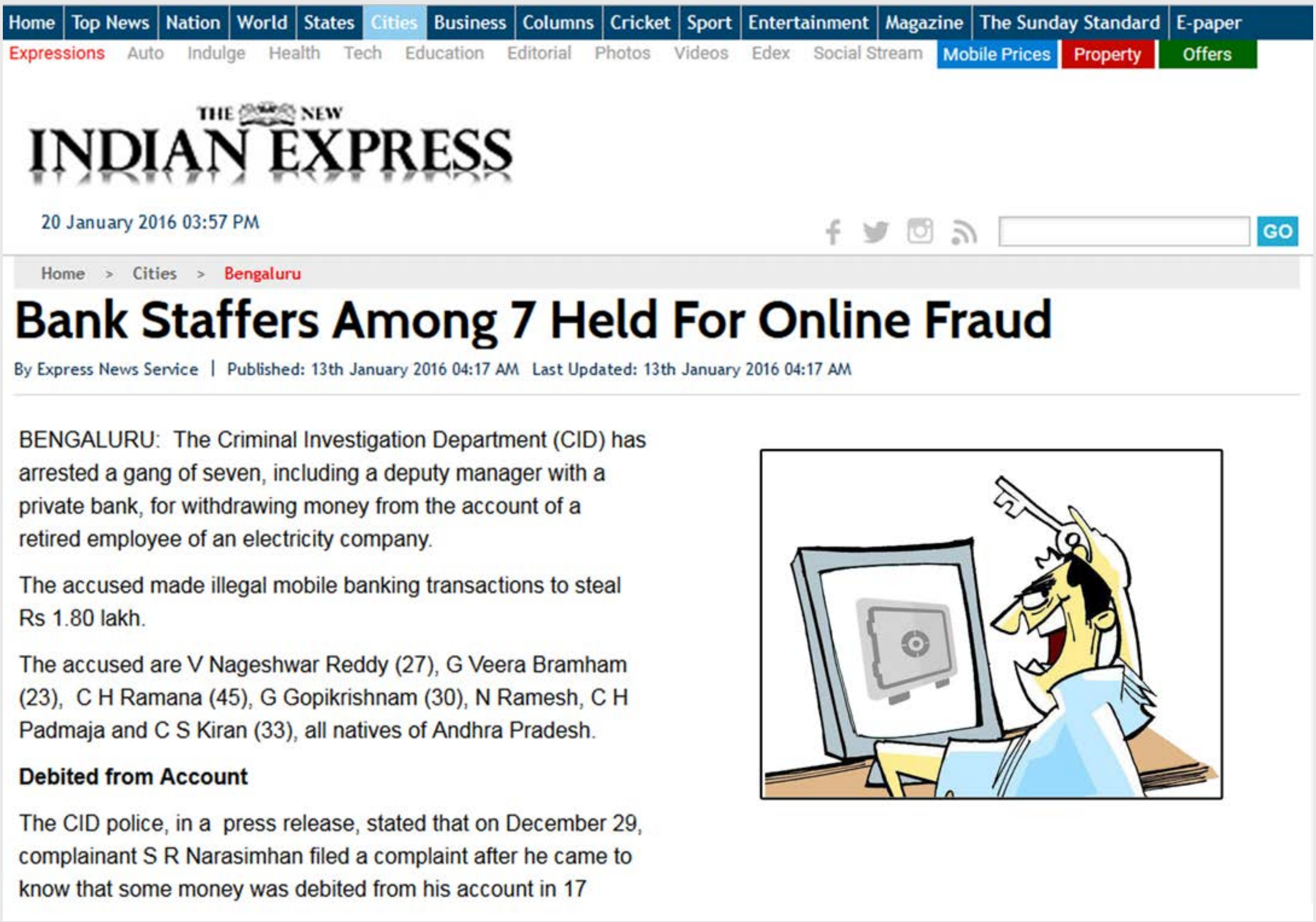
Categories

Reset all categories to: --Select--

Block	Adult/Mature	Block	Illegal Activities	Block	Proxy
Block	Alcohol	Block	Illegal Drugs	Allow	Social Networks
Block	Gambling	Block	Intimate Apparel/Swimsuits	Block	Tobacco
Block	Hate/Violence	Block	Pornography	Allow	Weapons

Mask Profanity Manage languages for profanity masking

Show me all 35 categories



20 January 2016 03:57 PM

Bank Staffers Among 7 Held For Online Fraud

By Express News Service | Published: 13th January 2016 04:17 AM Last Updated: 13th January 2016 04:17 AM

BENGALURU: The Criminal Investigation Department (CID) has arrested a gang of seven, including a deputy manager with a private bank, for withdrawing money from the account of a retired employee of an electricity company.

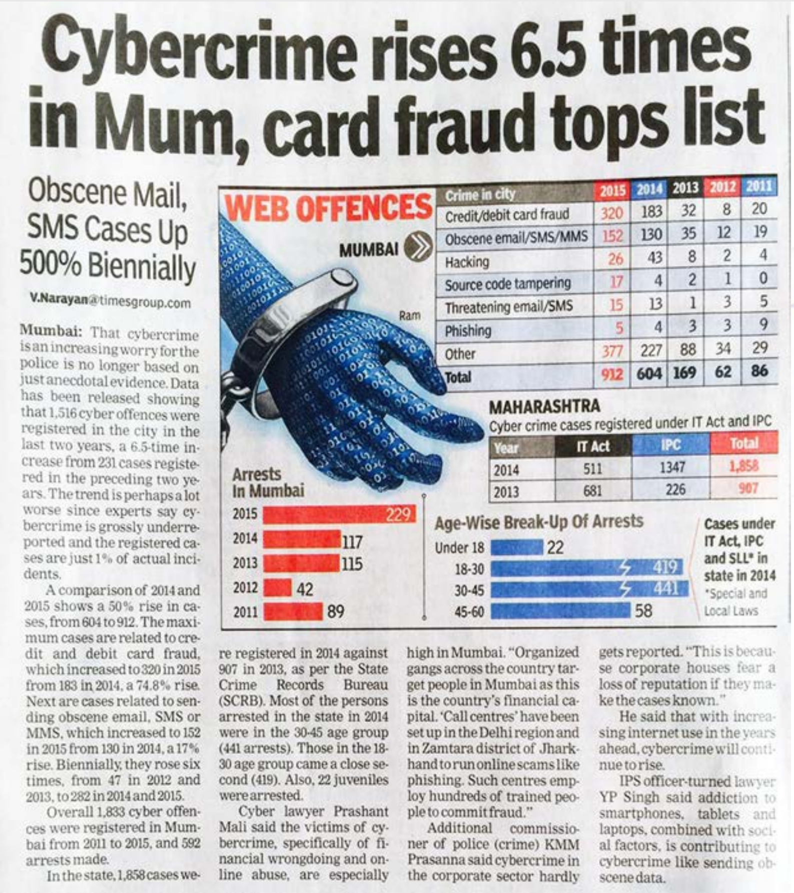
The accused made illegal mobile banking transactions to steal Rs 1.80 lakh.

The accused are V Nageshwar Reddy (27), G Veera Bramham (23), C H Ramana (45), G Gopikrishnam (30), N Ramesh, C H Padmaja and C S Kiran (33), all natives of Andhra Pradesh.

Debited from Account

The CID police, in a press release, stated that on December 29, complainant S R Narasimhan filed a complaint after he came to know that some money was debited from his account in 17

http://www.newindianexpress.com/cities/bengaluru/Bank-Staffers-Among-7-Held-For-Online-Fraud/2016/01/13/article3225511.ece



Cybercrime rises 6.5 times in Mum, card fraud tops list

Obscene Mail, SMS Cases Up 500% Biennially

V.Narayan@timesgroup.com

Mumbai: That cybercrime is an increasing worry for the police is no longer based on just anecdotal evidence. Data has been released showing that 1,516 cyber offences were registered in the city in the last two years, a 6.5-time increase from 231 cases registered in the preceding two years. The trend is perhaps a lot worse since experts say cybercrime is grossly underreported and the registered cases are just 1% of actual incidents.

A comparison of 2014 and 2015 shows a 50% rise in cases, from 604 to 912. The maximum cases are related to credit and debit card fraud, which increased to 320 in 2015 from 183 in 2014, a 74.8% rise. Next are cases related to sending obscene email, SMS or MMS, which increased to 152 in 2015 from 130 in 2014, a 17% rise. Biennially, they rose six times, from 47 in 2012 and 2013, to 282 in 2014 and 2015.

Overall 1,833 cyber offences were registered in Mumbai from 2011 to 2015, and 592 arrests made.

In the state, 1,858 cases were registered in 2014 against 907 in 2013, as per the State Crime Records Bureau (SCRB). Most of the persons arrested in the state in 2014 were in the 30-45 age group (441 arrests). Those in the 18-30 age group came a close second (419). Also, 22 juveniles were arrested.

Cyber lawyer Prashant Mali said the victims of cybercrime, specifically of financial wrongdoing and online abuse, are especially high in Mumbai. "Organized gangs across the country target people in Mumbai as this is the country's financial capital. 'Call centres' have been set up in the Delhi region and in Zamtara district of Jharkhand to run online scams like phishing. Such centres employ hundreds of trained people to commit fraud."

Additional commissioner of police (crime) KMM Prasanna said cybercrime in the corporate sector hardly gets reported. "This is because corporate houses fear a loss of reputation if they make the cases known."

He said that with increasing internet use in the years ahead, cybercrime will continue to rise.

IPS officer-turned lawyer YP Singh said addiction to smartphones, tablets and laptops, combined with social factors, is contributing to cybercrime like sending obscene data.

WEB OFFENCES

MUMBAI

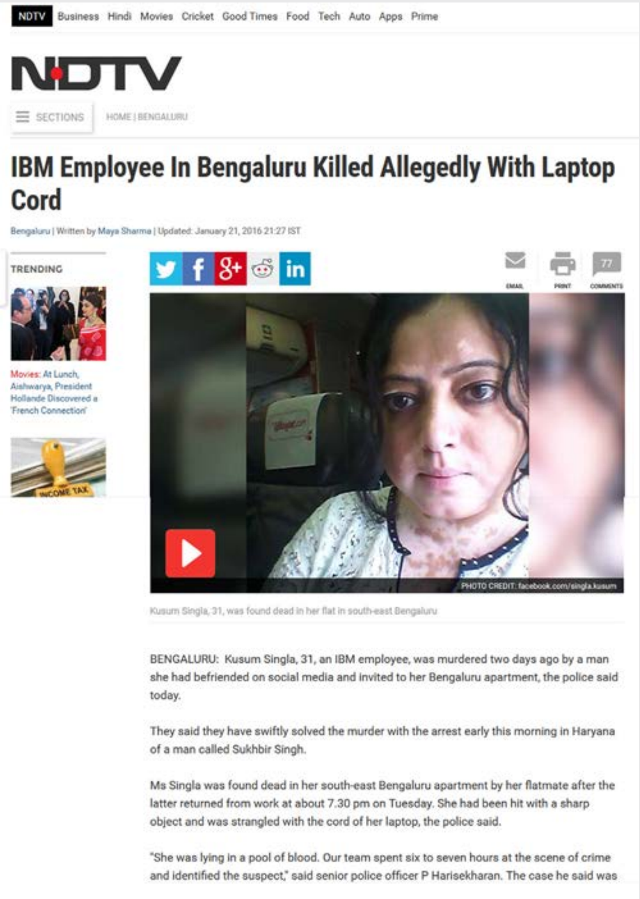
Crime in city	2015	2014	2013	2012	2011
Credit/debit card fraud	320	183	32	8	20
Obscene email/SMS/MMS	152	130	35	12	19
Hacking	26	43	8	2	4
Source code tampering	17	4	2	1	0
Threatening email/SMS	15	13	1	3	5
Phishing	5	4	3	3	9
Other	377	227	88	34	29
Total	912	604	169	62	86

MAHARASHTRA

Cyber crime cases registered under IT Act and IPC

Year	IT Act	IPC	Total
2014	511	1347	1,858
2013	681	226	907

http://timesofindia.indiatimes.com/city/mumbai/Cybercrime-rises-6-5-times-in-Mumbai-card-fraud-tops-list/articleshow/50576505.cms



IBM Employee In Bengaluru Killed Allegedly With Laptop Cord

Bengaluru | Written by Maya Sharma | Updated: January 21, 2016 21:27 IST

Kusum Singla, 31, was found dead in her flat in south-east Bengaluru

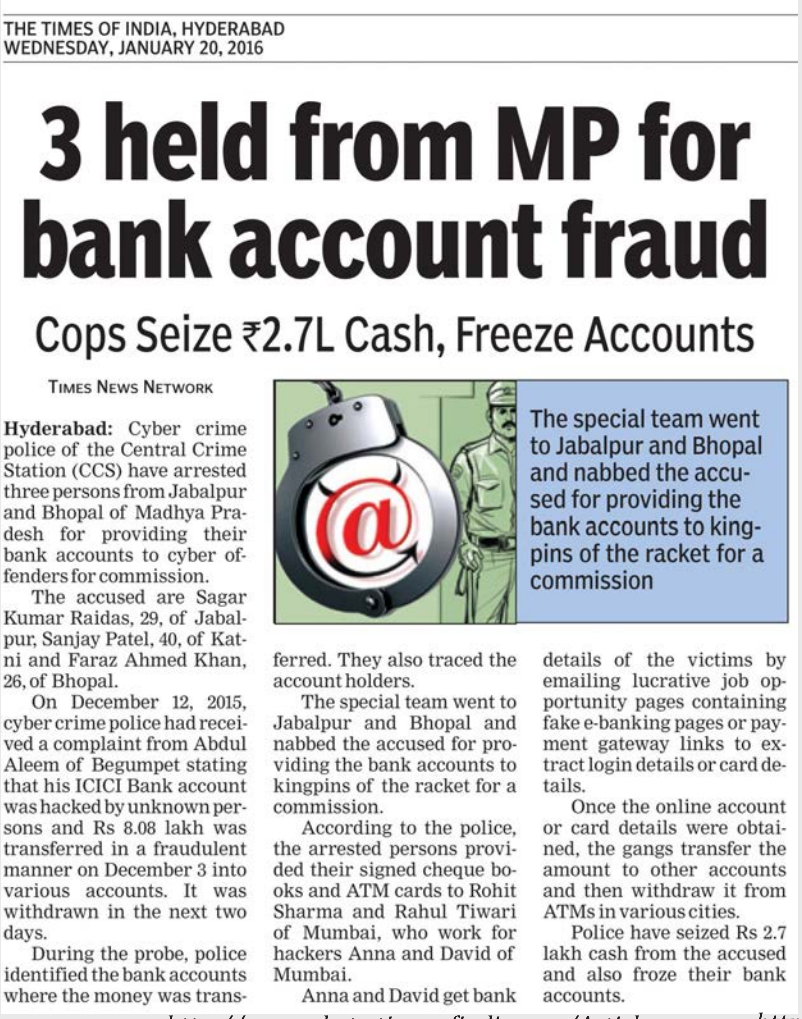
BENGALURU: Kusum Singla, 31, an IBM employee, was murdered two days ago by a man she had befriended on social media and invited to her Bengaluru apartment, the police said today.

They said they have swiftly solved the murder with the arrest early this morning in Haryana of a man called Sukhbir Singh.

Ms Singla was found dead in her south-east Bengaluru apartment by her flatmate after the latter returned from work at about 7.30 pm on Tuesday. She had been hit with a sharp object and was strangled with the cord of her laptop, the police said.

"She was lying in a pool of blood. Our team spent six to seven hours at the scene of crime and identified the suspect," said senior police officer P Harisekharan. The case he said was

http://www.ndtv.com/bangalore-news/ibm-employee-murdered-in-bengaluru-1268301?site=full



THE TIMES OF INDIA, HYDERABAD
WEDNESDAY, JANUARY 20, 2016

3 held from MP for bank account fraud

Cops Seize ₹2.7L Cash, Freeze Accounts

Times News Network

Hyderabad: Cyber crime police of the Central Crime Station (CCS) have arrested three persons from Jabalpur and Bhopal of Madhya Pradesh for providing their bank accounts to cyber offenders for commission.

The accused are Sagar Kumar Raidas, 29, of Jabalpur, Sanjay Patel, 40, of Katni and Faraz Ahmed Khan, 26, of Bhopal.

On December 12, 2015, cyber crime police had received a complaint from Abdul Aleem of Begumpet stating that his ICICI Bank account was hacked by unknown persons and Rs 8.08 lakh was transferred in a fraudulent manner on December 3 into various accounts. It was withdrawn in the next two days.

During the probe, police identified the bank accounts where the money was transferred. They also traced the account holders.

The special team went to Jabalpur and Bhopal and nabbed the accused for providing the bank accounts to kingpins of the racket for a commission.

According to the police, the arrested persons provided their signed cheque books and ATM cards to Rohit Sharma and Rahul Tiwari of Mumbai, who work for hackers Anna and David of Mumbai.

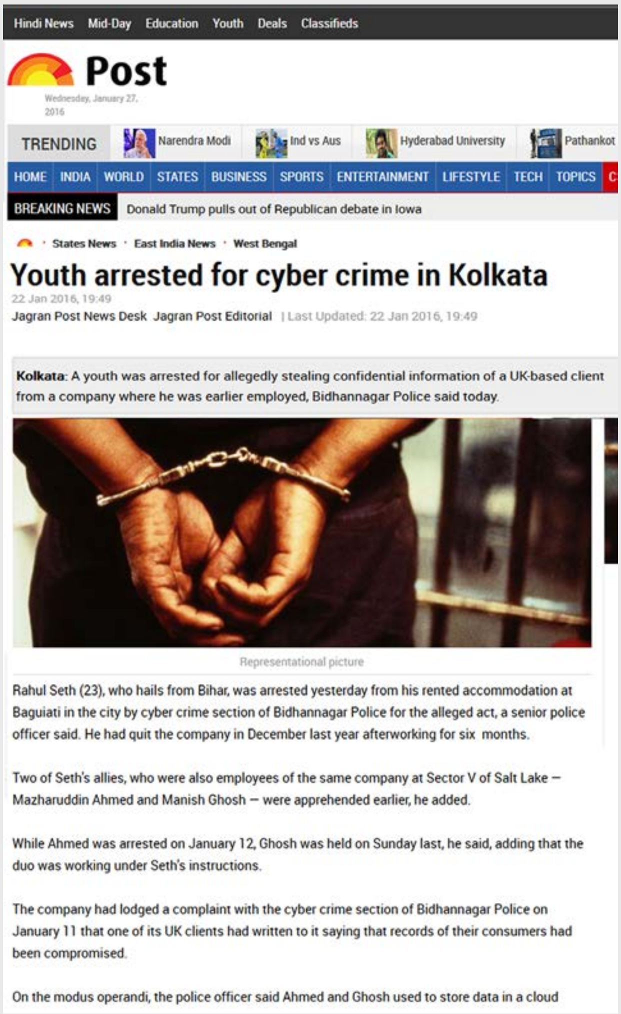
Anna and David get bank details of the victims by emailing lucrative job opportunity pages containing fake e-banking pages or payment gateway links to extract login details or card details.

Once the online account or card details were obtained, the gangs transfer the amount to other accounts and then withdraw it from ATMs in various cities.

Police have seized Rs 2.7 lakh cash from the accused and also froze their bank accounts.

The special team went to Jabalpur and Bhopal and nabbed the accused for providing the bank accounts to kingpins of the racket for a commission

http://epaperbeta.timesofindia.com/Article.aspx?eid=31809&articlexml=3-held-from-MP-for-bank-account-fraud-20012016005026



Hindi News Mid-Day Education Youth Deals Classifieds

Post

Wednesday, January 27, 2016

TRENDING Narendra Modi Ind vs Aus Hyderabad University Pathankot

HOME INDIA WORLD STATES BUSINESS SPORTS ENTERTAINMENT LIFESTYLE TECH TOPICS C

BREAKING NEWS Donald Trump pulls out of Republican debate in Iowa

States News · East India News · West Bengal

Youth arrested for cyber crime in Kolkata

22 Jan 2016, 19:49
Jagran Post News Desk Jagran Post Editorial | Last Updated: 22 Jan 2016, 19:49

Kolkata: A youth was arrested for allegedly stealing confidential information of a UK-based client from a company where he was earlier employed, Bidhannagar Police said today.

Representational picture

Rahul Seth (23), who hails from Bihar, was arrested yesterday from his rented accommodation at Baguiati in the city by cyber crime section of Bidhannagar Police for the alleged act, a senior police officer said. He had quit the company in December last year afterworking for six months.

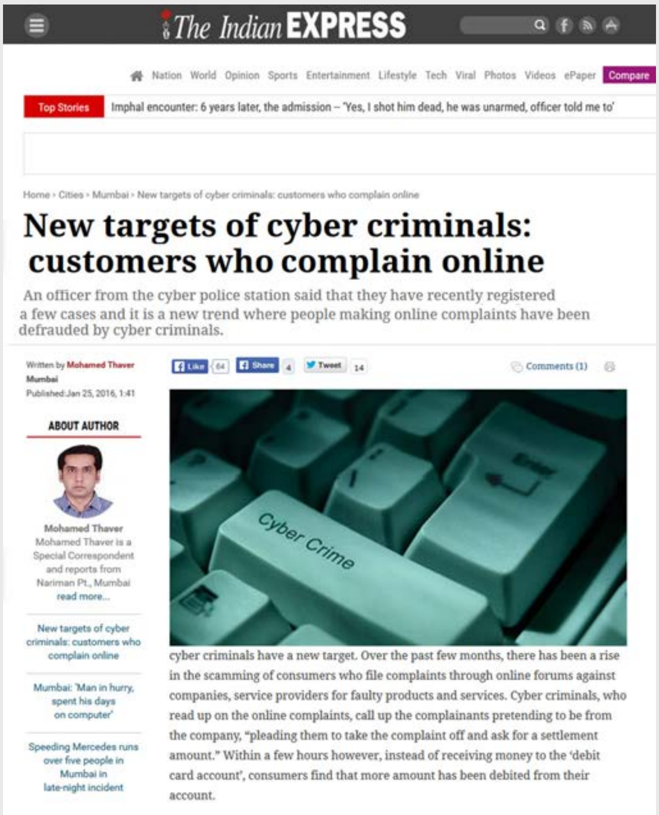
Two of Seth's allies, who were also employees of the same company at Sector V of Salt Lake – Mazharuddin Ahmed and Manish Ghosh – were apprehended earlier, he added.

While Ahmed was arrested on January 12, Ghosh was held on Sunday last, he said, adding that the duo was working under Seth's instructions.

The company had lodged a complaint with the cyber crime section of Bidhannagar Police on January 11 that one of its UK clients had written to it saying that records of their consumers had been compromised.

On the modus operandi, the police officer said Ahmed and Ghosh used to store data in a cloud

http://post.jagran.com/youth-arrested-for-cyber-crime-in-kolkata-1453472361



The Indian EXPRESS

Nation World Opinion Sports Entertainment Lifestyle Tech Viral Photos Videos ePaper Compare

Top Stories Imphal encounter: 6 years later, the admission – 'Yes, I shot him dead, he was unarmed, officer told me to'

Home › Cities › Mumbai › New targets of cyber criminals: customers who complain online

New targets of cyber criminals: customers who complain online

An officer from the cyber police station said that they have recently registered a few cases and it is a new trend where people making online complaints have been defrauded by cyber criminals.

Written by Mohamed Thaver
Mumbai
Published:Jan 25, 2016, 1:41

Like 64 Share 4 Tweet 14 Comments (1)

ABOUT AUTHOR

Mohamed Thaver
Mohamed Thaver is a Special Correspondent and reports from Nariman Pt., Mumbai
read more...

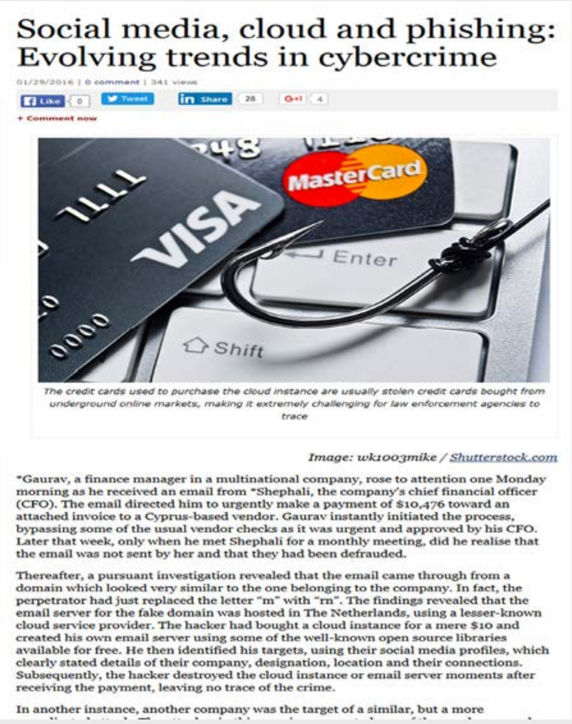
New targets of cyber criminals: customers who complain online

Mumbai: 'Man in hurry, spent his days on computer'

Speeding Mercedes runs over five people in Mumbai in late-night incident

cyber criminals have a new target. Over the past few months, there has been a rise in the scamming of consumers who file complaints through online forums against companies, service providers for faulty products and services. Cyber criminals, who read up on the online complaints, call up the complainants pretending to be from the company, "pleading them to take the complaint off and ask for a settlement amount." Within a few hours however, instead of receiving money to the 'debit card account', consumers find that more amount has been debited from their account.

http://indianexpress.com/article/cities/mumbai/new-targets-of-cyber-criminals-customers-who-complain-online/



Social media, cloud and phishing: Evolving trends in cybercrime

01/29/2016 | 0 comment | 341 views

Like 0 Tweet Share 28 G+1 4

+ Comment now

The credit cards used to purchase the cloud instance are usually stolen credit cards bought from underground online markets, making it extremely challenging for law enforcement agencies to trace

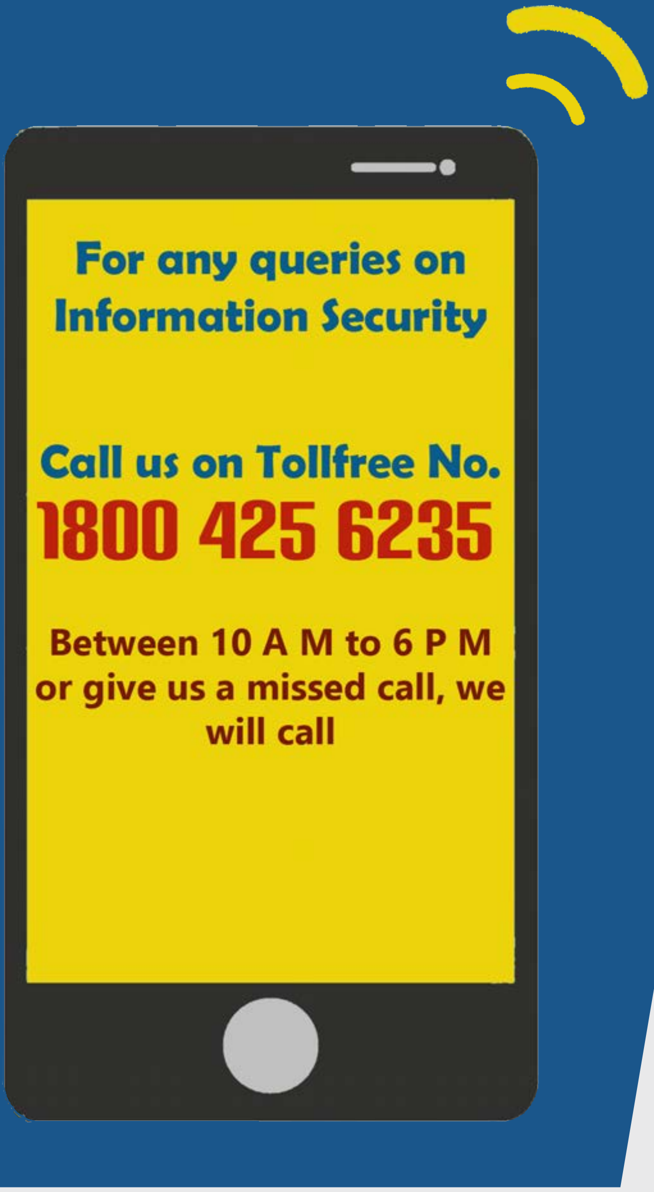
Image: wk1003mike / Shutterstock.com

*Gaurav, a finance manager in a multinational company, rose to attention one Monday morning as he received an email from *Shephali, the company's chief financial officer (CFO). The email directed him to urgently make a payment of $10,476 toward an attached invoice to a Cyprus-based vendor. Gaurav instantly initiated the process, bypassing some of the usual vendor checks as it was urgent and approved by his CFO. Later that week, only when he met Shephali for a monthly meeting, did he realise that the email was not sent by her and that they had been defrauded.

Thereafter, a pursuant investigation revealed that the email came through from a domain which looked very similar to the one belonging to the company. In fact, the perpetrator had just replaced the letter "m" with "rn". The findings revealed that the email server for the fake domain was hosted in The Netherlands, using a lesser-known cloud service provider. The hacker had bought a cloud instance for a mere $10 and created his own email server using some of the well-known open source libraries available for free. He then identified his targets, using their social media profiles, which clearly stated details of their company, designation, location and their connections. Subsequently, the hacker destroyed the cloud instance or email server moments after receiving the payment, leaving no trace of the crime.

In another instance, another company was the target of a similar, but a more

http://forbesindia.com/blog/economy-policy/social-media-cloud-and-phishing-evolving-trends-in-cybercrime/#ixzz3yyNS4FIz



For any queries on Information Security

Call us on Tollfree No.

1800 425 6235

Between 10 A M to 6 P M or give us a missed call, we will call

To share tips / Latest news mail us to
pmu-isea@cdac.in

Follow us on Facebook
https://www.facebook.com/infosecawarenesss

Follow us on Youtube
https://www.youtube.com/channel/UCWPBKQryyVvydUy4rYsbBfA

Follow us on twitter
https://twitter.com/CDAC_ISEA

For more details visit
www.infosecawareness.in

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India, is primarily an R&D institution involved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded programming in the application domains of Network Security, e-learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain Management and Wireless Sensor Networks.

सत्यमेव जयते

Department of Electronics & Information Technology,
Ministry of Comunications & Information Technology,
Government of India

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India

Nalanda Building, No. 1 Shivabagh Satyam Theatre Road,
Ameerpet, Hyderabad - 500016, Telangana (India)

Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway,
Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 500005, Telangana(India)

E-mail : isea@cdac.in