



Case Studies on Recent Cyber Attacks

Presentation by:

Cyber Security Centre of Excellence (CS-CoE)

Department of Information Technology & Electronics, Government of West Bengal



Landmark Cyber Attacks / Breaches

AUG 2019

Bihar education department website hacked

- ❑ The official website of the Bihar Education Department was hacked on Sunday, with hackers uploading messages in praise of Pakistan on the webpage.
- ❑ "RootAyyildiz Turkish Hacker" claimed responsibility for hacking the website and posted messages in praise of Pakistan and Islam.
- ❑ Soon after, the website was not accessible and displayed- Service Unavailable. HTTP Error 503 message.

OCT 2019

Kudankulum cyber attack

- ❑ The investigation revealed that the infected PC belonged to a user who was connected in the internet connected network used for administrative purposes. This is isolated from the critical internal network
- ❑ Identification of malware in NPCIL system
- ❑ Dtrack malware - A Spyware in ATM Machines and Company Servers Can Steal Your Money and Data

MAY 2018

Data theft at zomato

- ❑ The food tech company discovered that data, including names, email IDs and hashed passwords, of 17 million users was stolen by an 'ethical' hacker-who demanded the company must acknowledge its security vulnerabilities and put up for sale on the Dark Web

FEB 2019

24 websites of central ministries, departments and state governments were hacked

- ❑ "As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 199, 172, 110 and 25 **websites of Central Ministries/Departments and State Governments were hacked** during the year 2016, 2017, 2018 and 2019 (**till May**)



Hackers steal Rs. 1.5 Lakh from card without OTP, PIN

Bank says they are investing the case.....

Nothing has happened even after 20 days.

All the hacker needs is card number and CVV. Skimming is a method used by identity thieves to capture information from a cardholder.

- Fraudsters often use a device called a skimmer that can be installed at gas pumps or ATM machines to collect card data.
- Some machines act like point-of-sale technology. An acquired card is swiped, and a touch pad allows the user to enter a security code.
- Card users are warned to keep their cards in their sight at all times and to cover the pin pad when inputting security codes



Turkish cybercriminals hack Tripura ATMs, steal huge cash

According to the police, banks and other sources, over 60 bank customers of different banks mostly State Bank of India (SBI) during the past few days lost lakhs of rupees due to the fraudulent acts of the cybercriminals and ATM hackers

Over Rs 80 lakhs of several customers were stolen from several ATMs during the past few days in Agartala

According to a cyber-technology expert, the ATM card cloning system comprises a spy camera, a memory card and a small data device to gather ATM and account details of bank customers.

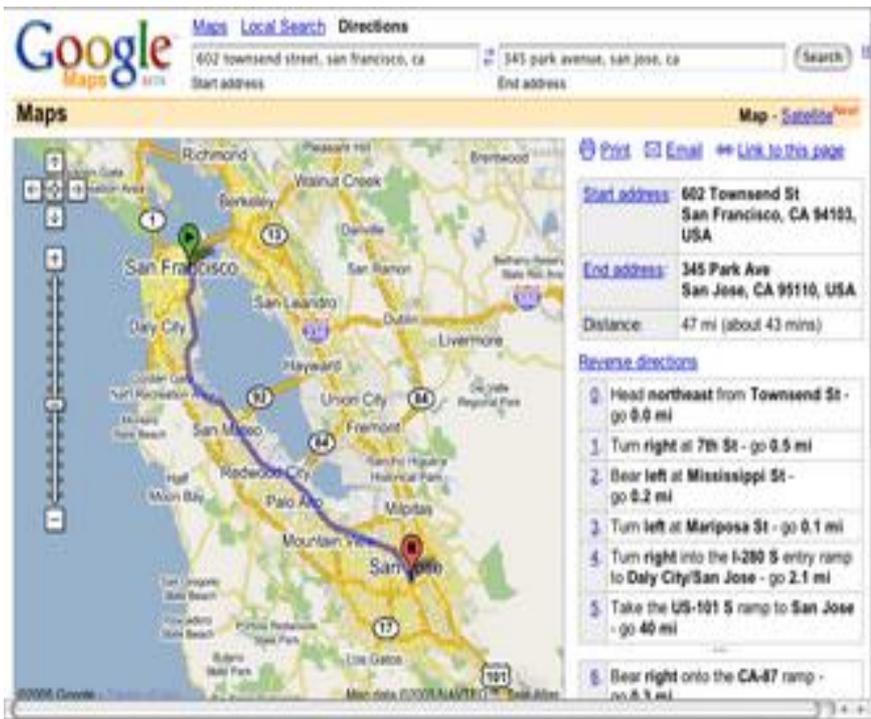
Seventh Pay Commission: Know how Pak based cyber attackers lured Indian govt. officials

Pak group uses 7th Pay Commission to target Indian govt officials: FireEye

Pay Matrix (Defence Forces Personnel - Except SDNS)

Pay Band	G-15 (A)					G-16 (A)					G-17 (A)					G-18 (A)					Special Pay	Dearness Allowance	Gratuity																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																						
Grade Pay	200	250	300	350	400	450	500	550	600	650	700	750	800	850	900	950	1000	1050	1100	1150	1200	1250	1300	1350	1400	1450	1500	1550	1600	1650	1700	1750	1800	1850	1900	1950	2000	2050	2100	2150	2200	2250	2300	2350	2400	2450	2500	2550	2600	2650	2700	2750	2800	2850	2900	2950	3000	3050	3100	3150	3200	3250	3300	3350	3400	3450	3500	3550	3600	3650	3700	3750	3800	3850	3900	3950	4000	4050	4100	4150	4200	4250	4300	4350	4400	4450	4500	4550	4600	4650	4700	4750	4800	4850	4900	4950	5000	5050	5100	5150	5200	5250	5300	5350	5400	5450	5500	5550	5600	5650	5700	5750	5800	5850	5900	5950	6000	6050	6100	6150	6200	6250	6300	6350	6400	6450	6500	6550	6600	6650	6700	6750	6800	6850	6900	6950	7000	7050	7100	7150	7200	7250	7300	7350	7400	7450	7500	7550	7600	7650	7700	7750	7800	7850	7900	7950	8000	8050	8100	8150	8200	8250	8300	8350	8400	8450	8500	8550	8600	8650	8700	8750	8800	8850	8900	8950	9000	9050	9100	9150	9200	9250	9300	9350	9400	9450	9500	9550	9600	9650	9700	9750	9800	9850	9900	9950	10000	10050	10100	10150	10200	10250	10300	10350	10400	10450	10500	10550	10600	10650	10700	10750	10800	10850	10900	10950	11000	11050	11100	11150	11200	11250	11300	11350	11400	11450	11500	11550	11600	11650	11700	11750	11800	11850	11900	11950	12000	12050	12100	12150	12200	12250	12300	12350	12400	12450	12500	12550	12600	12650	12700	12750	12800	12850	12900	12950	13000	13050	13100	13150	13200	13250	13300	13350	13400	13450	13500	13550	13600	13650	13700	13750	13800	13850	13900	13950	14000	14050	14100	14150	14200	14250	14300	14350	14400	14450	14500	14550	14600	14650	14700	14750	14800	14850	14900	14950	15000	15050	15100	15150	15200	15250	15300	15350	15400	15450	15500	15550	15600	15650	15700	15750	15800	15850	15900	15950	16000	16050	16100	16150	16200	16250	16300	16350	16400	16450	16500	16550	16600	16650	16700	16750	16800	16850	16900	16950	17000	17050	17100	17150	17200	17250	17300	17350	17400	17450	17500	17550	17600	17650	17700	17750	17800	17850	17900	17950	18000	18050	18100	18150	18200	18250	18300	18350	18400	18450	18500	18550	18600	18650	18700	18750	18800	18850	18900	18950	19000	19050	19100	19150	19200	19250	19300	19350	19400	19450	19500	19550	19600	19650	19700	19750	19800	19850	19900	19950	20000	20050	20100	20150	20200	20250	20300	20350	20400	20450	20500	20550	20600	20650	20700	20750	20800	20850	20900	20950	21000	21050	21100	21150	21200	21250	21300	21350	21400	21450	21500	21550	21600	21650	21700	21750	21800	21850	21900	21950	22000	22050	22100	22150	22200	22250	22300	22350	22400	22450	22500	22550	22600	22650	22700	22750	22800	22850	22900	22950	23000	23050	23100	23150	23200	23250	23300	23350	23400	23450	23500	23550	23600	23650	23700	23750	23800	23850	23900	23950	24000	24050	24100	24150	24200	24250	24300	24350	24400	24450	24500	24550	24600	24650	24700	24750	24800	24850	24900	24950	25000	25050	25100	25150	25200	25250	25300	25350	25400	25450	25500	25550	25600	25650	25700	25750	25800	25850	25900	25950	26000	26050	26100	26150	26200	26250	26300	26350	26400	26450	26500	26550	26600	26650	26700	26750	26800	26850	26900	26950	27000	27050	27100	27150	27200	27250	27300	27350	27400	27450	27500	27550	27600	27650	27700	27750	27800	27850	27900	27950	28000	28050	28100	28150	28200	28250	28300	28350	28400	28450	28500	28550	28600	28650	28700	28750	28800	28850	28900	28950	29000	29050	29100	29150	29200	29250	29300	29350	29400	29450	29500	29550	29600	29650	29700	29750	29800	29850	29900	29950	30000	30050	30100	30150	30200	30250	30300	30350	30400	30450	30500	30550	30600	30650	30700	30750	30800	30850	30900	30950	31000	31050	31100	31150	31200	31250	31300	31350	31400	31450	31500	31550	31600	31650	31700	31750	31800	31850	31900	31950	32000	32050	32100	32150	32200	32250	32300	32350	32400	32450	32500	32550	32600	32650	32700	32750	32800	32850	32900	32950	33000	33050	33100	33150	33200	33250	33300	33350	33400	33450	33500	33550	33600	33650	33700	33750	33800	33850	33900	33950	34000	34050	34100	34150	34200	34250	34300	34350	34400	34450	34500	34550	34600	34650	34700	34750	34800	34850	34900	34950	35000	35050	35100	35150	35200	35250	35300	35350	35400	35450	35500	35550	35600	35650	35700	35750	35800	35850	35900	35950	36000	36050	36100	36150	36200	36250	36300	36350	36400	36450	36500	36550	36600	36650	36700	36750	36800	36850	36900	36950	37000	37050	37100	37150	37200	37250	37300	37350	37400	37450	37500	37550	37600	37650	37700	37750	37800	37850	37900	37950	38000	38050	38100	38150	38200	38250	38300	38350	38400	38450	38500	38550	38600	38650	38700	38750	38800	38850	38900	38950	39000	39050	39100	39150	39200	39250	39300	39350	39400	39450	39500	39550	39600	39650	39700	39750	39800	39850	39900	39950	40000	40050	40100	40150	40200	40250	40300	40350	40400	40450	40500	40550	40600	40650	40700	40750	40800	40850	40900	40950	41000	41050	41100	41150	41200	41250	41300	41350	41400	41450	41500	41550	41600	41650	41700	41750	41800	41850	41900	41950	42000	42050	42100	42150	42200	42250	42300	42350	42400	42450	42500	42550	42600	42650	42700	42750	42800	42850	42900	42950	43000	43050	43100	43150	43200	43250	43300	43350	43400	43450	43500	43550	43600	43650	43700	43750	43800	43850	43900	43950	44000	44050	44100	44150	44200	44250	44300	44350	44400	44450	44500	44550	44600	44650	44700	44750	44800	44850	44900	44950	45000	45050	45100	45150	45200	45250	45300	45350	45400	45450	45500	45550	45600	45650	45700	45750	45800	45850	45900	45950	46000	46050	46100	46150	46200	46250	46300	46350	46400	46450	46500	46550	46600	46650	46700	46750	46800	46850	46900	46950	47000	47050	47100	47150	47200	47250	47300	47350	47400	47450	47500	47550	47600	47650	47700	47750	47800	47850	47900	47950	48000	48050	48100	48150	48200	48250	48300	48350	48400	48450	48500	48550	48600	48650	48700	48750	48800	48850	48900	48950	49000	49050	49100	49150	49200	49250	49300	49350	49400	49450	49500	49550	49600	49650	49700	49750	49800	49850	49900	49950	50000	50050	50100	50150	50200	50250	50300	50350	50400	50450	50500	50550	50600	50650	50700	50750	50800	50850	50900	50950	51000	51050	51100	51150	51200	51250	51300	51350	51400	51450	51500	51550	51600	51650	51700	51750	51800	51850	51900	51950	52000	52050	52100	52150	52200	52250	52300	52350	52400	52450	52500	52550	52600	52650	52700	52750	52800	52850	52900	52950	53000	53050	53100	53150	53200	53250	53300	53350	53400	53450	53500	53550	53600	53650	53700	53750	53800	53850	53900	53950	54000	54050	54100	54150	54200	54250	54300	54350	54400	54450	54500	54550	54600	54650	54700	54750	54800	54850	54900	54950	55000	55050	55100	55150	55200	55250	55300	55350	55400	55450	55500	55550	55600	55650	55700	55750	55800	55850	55900	55950	56000	56050	56100	56150	56200	56250	56300	56350	56400	56450	56500	56550	56600	56650	56700	56750	56800	56850	56900	56950	57000	57050	57100	57150	57200	57250	57300	57350	57400	57450	57500	57550	57600	57650	57700	57750	57800	57850	57900	57950	58000	58050	58100	58150	58200	58250	58300	58350	58400	58450	58500	58550	58600	58650	58700	58750	58800	58850	58900	58950	59000	59050	59100	59150	59200	59250	59300	59350	59400	59450	59500	59550	59600	59650	59700	59750	59800	59850	59900	59950	60000	60050	60100	60150	60200	60250	60300	60350	60400	60450	60500	60550	60600	60650	60700	60750	60800	60850	60900	60950	61000	61050	61100	61150	61200	61250	61300	61350	61400	61450	61500	61550	61

What happens if you post your photograph on Facebook? Data Privacy issues... Do You have a Social Media Policy?



ISI laying honeytraps on Facebook and Twitter to snare Indian defence personnel

Fake Facebook profile, chats through WhatsApp: How suspected ISI agent 'honey-trapped' Army personnel



Co – Op Bank Attack -- Events..

xxth August – 20xx – ATM attack

- ❖ **2.30 PM received a call** – Large number of Transactions are **Declining**
- ❖ **3.30 PM received a call** – Large number of transactions are **Approved & Declining**
- ❖ **5.30 PM received a call** – Large number of Transaction are **Approved.**
- ❖ **5.47 PM Bank Disconnected Switch with VISA switch** – All Internationals transactions gets stopped.
- ❖ **6.00 PM received a call from Indian Customer** – Random Balance Amount, No checking, Accepting Wrong Pin...
- ❖ **8.00 PM, disconnected the NPCI Switch**
- ❖ **Rs. Xxxx + Crores lost; xxxx + Fraudulent Transactions.**
- ❖ Same Card, different Countries, number of Transactions, Velocity Check(?)
- ❖ **Bank not aware about the transactions...**

Co-operative Bank's...

1

The attackers used spear-phishing mails for the initial compromise of the systems

2

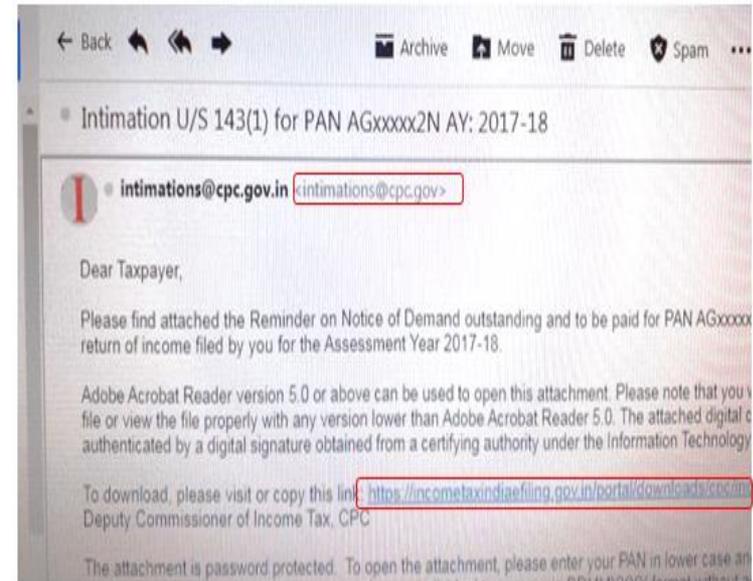
Installed Keylogging and Remote Access Tool's on the compromised systems

3

Stolen the authentication credentials & digital certificates

4

Performed fraudulent transactions from external IP addresses using stolen digital certificates





Ransomware - advanced type of malware that restricts access to the computer system until the user pays a fee

Malware - malicious software. Piece of software written with the intent of damaging devices, stealing data. Viruses, Spyware and Ransomware are among the different kinds of malware

Pegasys - Pegasus is capable of reading text messages, tracking calls, collecting passwords, tracing the location of the phone, accessing the target device's microphone(s) and video camera(s), and gathering information from apps.

Honeytrap - Honey trapping is an investigative practice involving the use of romantic relationships for interpersonal, political or monetary purpose.



Dark Web - part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable



How many of you check... Hardware Key-Logger Do you have a Data Leakage Prevention Policy?



KeyGhost Tutorial step-by-step - Netscape

1 / 10 : Install KeyGhost or Security Keyboard

Install KeyGhost on Target Computer

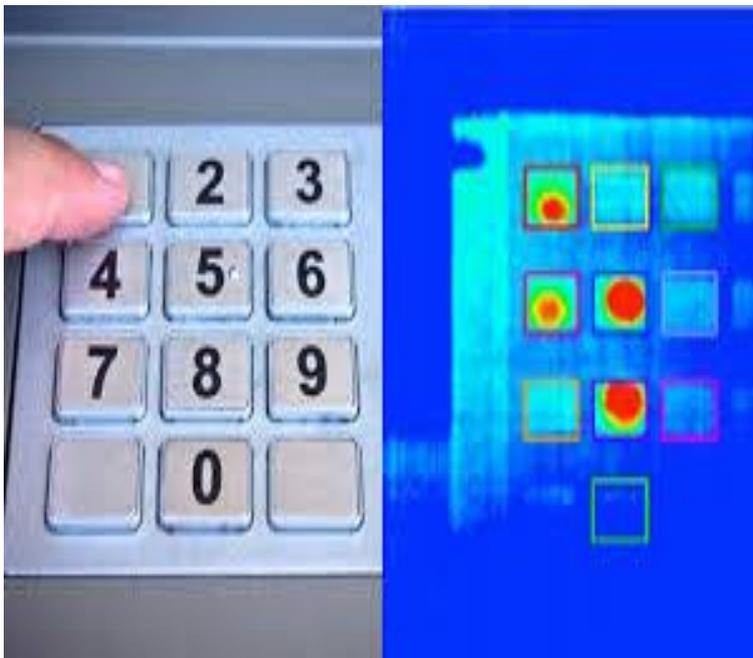
Before	After
	
KeyGhost™ installs even when computer is logged out, password protected or turned off.	The unique operation of KeyGhost™ means that <i>you never need to install any software at all.</i>

Tutorial: how to use KeyGhost < Back Next >

1. Don't leave computer unattended with sensitive information on screen
2. Always lock your computer when leaving it unattended with "windows + L" or "ctrl+alt+del"
3. Make sure all vendor updates to the applications/ software you are using is getting updated on a regular basis

2013 Incident

- Which ATM better – First PIN or Last PIN
- Plastic buttons or Metal buttons?



1. Do not share your credit/debit card number, CVV2 code or PIN with anyone
2. When making online payments, make sure that the green padlock and https symbols are active and valid. Do not enter card details in any unverified website/ application or portal
3. When using card in ATM or POS machines, ensure that the device where the card is being used has not been tampered with.



Form Grabbing – Spam Mail filtering....

The image shows the Spy Eye web interface. At the top, there is a large eye icon and the text "Spy Eye". Below this, there are several navigation buttons: "Find INFO", "Statistic", "FTP accounts", "Settings", and "Screen shots". A clock shows the time as 15:32:51. On the right, there is a status bar showing "3476 k" and "+395093".

The main section is titled "Get Screenshots" and contains a form with the following fields:

- Bot GUID :
- Report date region :
- Limit :
-

Below the form, there is a preview of a screenshot. The screenshot shows a keyboard layout with a mouse cursor over the 't' key. The URL at the bottom of the screenshot is <https://www.libertyreserve.com/en/customer/login?index.aspx>. The date "11/4/2010" is displayed above the screenshot.

1. Always use genuine vendor software and operating system
2. Always use password protection for your laptop/ mobile device
3. Always use licensed anti-virus software
4. Do not download any software from untrusted sources
5. Do not keep any applications or software which you do not regularly use

Thank you