Cyber Crimes

Understanding Cyber Security &

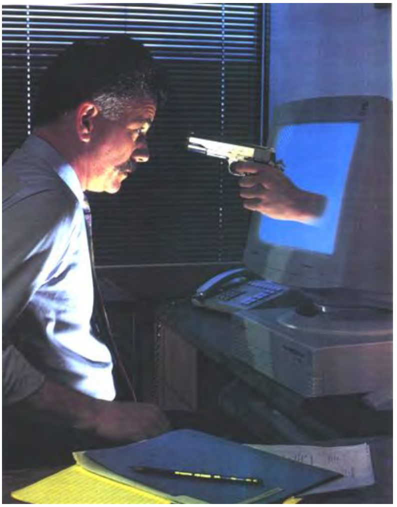
Presented by: Idris Ismaila, PhD

ismi.idris@futminna.edu.ng

A Presentation at the 1st Nigeria Computer Society (NCS) Workshop on Cybercrime Detection and Forensic Investigation. 26th -28th May, 2021

Cybersecurity vs. Cyber-Crime

- Cybersecurity
  - Protection of assets against risks within, and from, the electronic environment



- Cyber-Crime
  - Conduct prohibited by law, with prescribed punishment, carried out using digital systems like computers, electronic, ancillary devices, processes and/ or procedures
  - Criminality is the state of being illegal

Cyber-criminals operate at the speed of light while law enforcement moves at the speed of law.

Risk

- The core duty of cybersecurity is to identify, mitigate and manage cyber risk to an organization’s digital assets.

- it is important to understand risk in the context of cybersecurity, which means knowing how to determine, measure and reduce risk effectively.

Assessing Risk..

- Assessing risk is one of the most critical functions of a cybersecurity organization.

- Effective policies, security implementations, resource allocation and incident response preparedness are all dependent on understanding the risk and threats an organization faces.

- If controls are not implemented based on awareness of actual risk, then valuable organizational assets will not be adequately protected while other assets will be wastefully overprotected.

Approaches to Cybersecurity

- **Compliance-based**—Also known as standards-based security, this approach relies on regulations or standards to determine security implementations. Controls are implemented regardless of their applicability or necessity, which often leads to a "checklist" attitude toward security.

- **Risk-based**—Risk-based security relies on identifying the unique risk a particular organization faces and designing and implementing security controls to address that risk above and beyond the entity's risk tolerance and business needs.

- ***Ad hoc***—An *ad hoc* approach simply implements security with no particular rationale or criteria. Ad hoc implementations may be driven by vendor marketing, or they may reflect insufficient subject matter expertise, knowledge or training when designing and implementing safeguards.

Key Terms and Definitions

- **Risk**—The combination of the probability of an event and its consequence (International Organization for Standardization/International Electrotechnical Commission [ISO/IEC]). Risk is mitigated through the use of controls or safeguards.

- **Threat**—Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm. ISO/IEC 13335 defines a threat broadly as a potential cause of an unwanted incident. Some organizations make a further distinction between a threat source and a threat event, classifying a threat source as the actual process or agent attempting to cause harm, and a threat event as the result or outcome of a threat agent's malicious activity.

- **Asset**—Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation

- **Vulnerability**—A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events.

Specific Types of Risk That Apply to Cybersecurity

- **Residual risk**—Even after safeguards are in place, there will always be residual risk, defined as the remaining risk after management has implemented a risk response.

- **Inherent risk**—The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)

- **Likelihood and Impact**

When assessing a threat, cybersecurity professionals often analyze the threat's likelihood and impact in order to rank and prioritize it among other existing threats.

What is Cyber Security?

- Cyber Security is the process and techniques involved in protecting sensitive data, computer systems, networks and software applications from cyber attacks. The cyber attacks are general terminology which covers a large number of topics, but some of the popular are:

- Tampering systems and data stored within
- Exploitation of resources
- Unauthorized access to the targeted system and accessing sensitive information
- Disrupting normal functioning of the business and its processes
- Using ransomware attacks to encrypt data and extort money from victims

The key concept of Cyber Security?

- The Cyber Security on a whole is a very broad term but is based on three fundamental concepts known as “**The CIA Triad**“.

- It consists of Confidentiality, Integrity and Availability. This model is designed to guide the organization with the policies of Cyber Security in the realm of Information security.

Confidentiality

- It defines the rules that limits the access of information. Confidentiality takes on the measures to restrict the sensitive information from being accessed by cyber attackers and hackers.
- In an organization, peoples are allowed or denied the access of information according to its category by authorizing the right persons in a department. They are also given proper training about the sharing of information and securing their accounts with strong passwords.

Integrity

- This assures that the data is consistent, accurate and trustworthy over its time period. It means that the data within the transit should not be changed, altered, deleted or illegally being accessed.

- Proper measures should be taken in an organization to ensure its safety. File permissions and user access control are the measures controlling the data breach. Also, there should be tools and technologies implemented to detect any change or breach in the data. Various Organizations uses a checksum, and even cryptographic checksum to verify the integrity of data.

Availability

- Availability in terms of all necessary components like hardware, software, networks, devices and security equipment should all be maintained and upgraded. This will ensure the smooth functioning and access of Data without any disruption. Also providing constant communication between the components through providing enough bandwidth.

Why is Cyber Crime Important?

- 97 Millions Internet users in Nigeria (NCC)
- Nigeria lost N15 billion to cyber crime in 2019 (EFCC)
- Crimes like forgery, extortion, kidnapping , are all being assisted online
- You are able to monitor all transactions online

Definition of a cyber crime

- Computer crime, or cybercrime, is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.
- Computer crime is when
  - Computer is a target
  - Computer is a tool for the crime
  - Computer is incidental to a crime

The Usual Suspects

- Disgruntled employees
- Teenagers
- Political activist
- Professional Hackers
- Business Rival
- Ex wife or husband/BF or GF
- Rogue Nations

Usual Victims

- Gullible
- Greedy people
- Unskilled and Inexperienced
- Trusting People
- Unlucky people
- Organizations
- As a matter of fact anybody

Motives

- Financial gains
- Intellectual property (espionage)
- Political (hacktivism)

Recent Patterns in the cyber crime

- Hackers are more sophisticated in their attacks and use of tools.
- Attack patterns are now being applied to mobile devices.
- Multiple nation states have the capabilities to infiltrate government and private targets (cyberwarfare).
- Cloud computing results in large concentrations of data within a small number of facilities
- Social networks have become a primary channel for communication, knowledge collection, marketing and dissemination of information.
- Big data refers to large collections of structured and unstructured data and the usage of large infrastructure, applications, web services and device

Why are the bad guys winning?

- Anonymity of Internet
- Jurisdiction issue
- Cyber crime is under reported
- Law enforcement are ill equipped
- Lack of Awareness from user

Trends in Cyber Crimes Methodology

- Hacking
- Denial of service attack
- Malware dissemination
- Software Piracy
- Pornography
- IRC Crimes
- Credit Card Fraud
- NET Extortion
- Phishing
- Spoofing
- Cyber Stalking
- Cyber Defamation
- Threatening
- Terrorism
- Salami Attack

Hacking

Hacking

- Hacking: Illegal intrusion into a computer system without the permission of the computer owner/user
- The criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

Types of Hacking

- Website Hacking
- Email hacking
- Network Hacking
- Password Hacking
- Online Banking Hacking
- Computer Hacking
- Wireless Access Hacking

Social Engineering

- **Social engineering** is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter.

Social Engineering

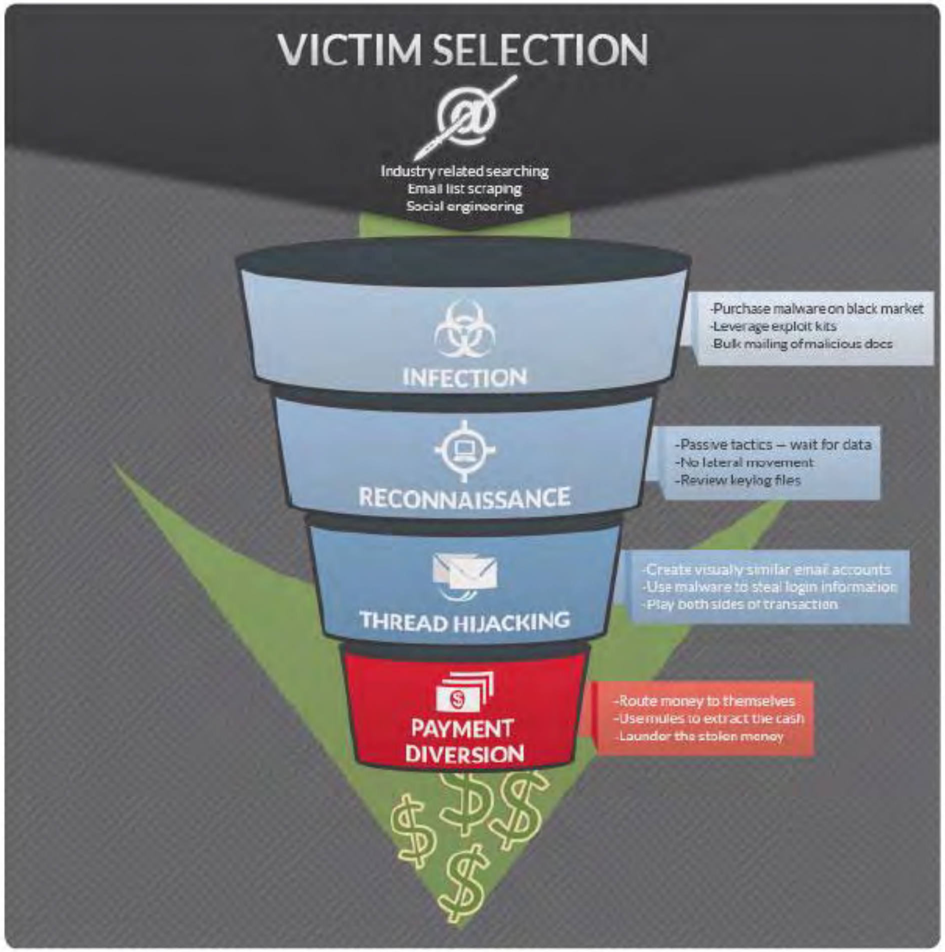
Denial of Service Attack

- An act by the criminal, who floods the bandwidth of the victim's network or fills their e-mail box with spam mail depriving him of the services he is entitled to access or provide

Malware Dissemination

- Malicious software that attaches itself to other software.
- (Virus, Worms, Trojan Horse, Time Bomb, Logic Bomb)

Malware – Overview of Nig Group



VICTIM SELECTION

Industry related searching
Email list scraping
Social engineering

INFECTION

-Purchase malware on black market
-Leverage exploit kits
-Bulk mailing of malicious docs

RECONNAISSANCE

-Passive tactics – wait for data
-No lateral movement
-Review keylog files

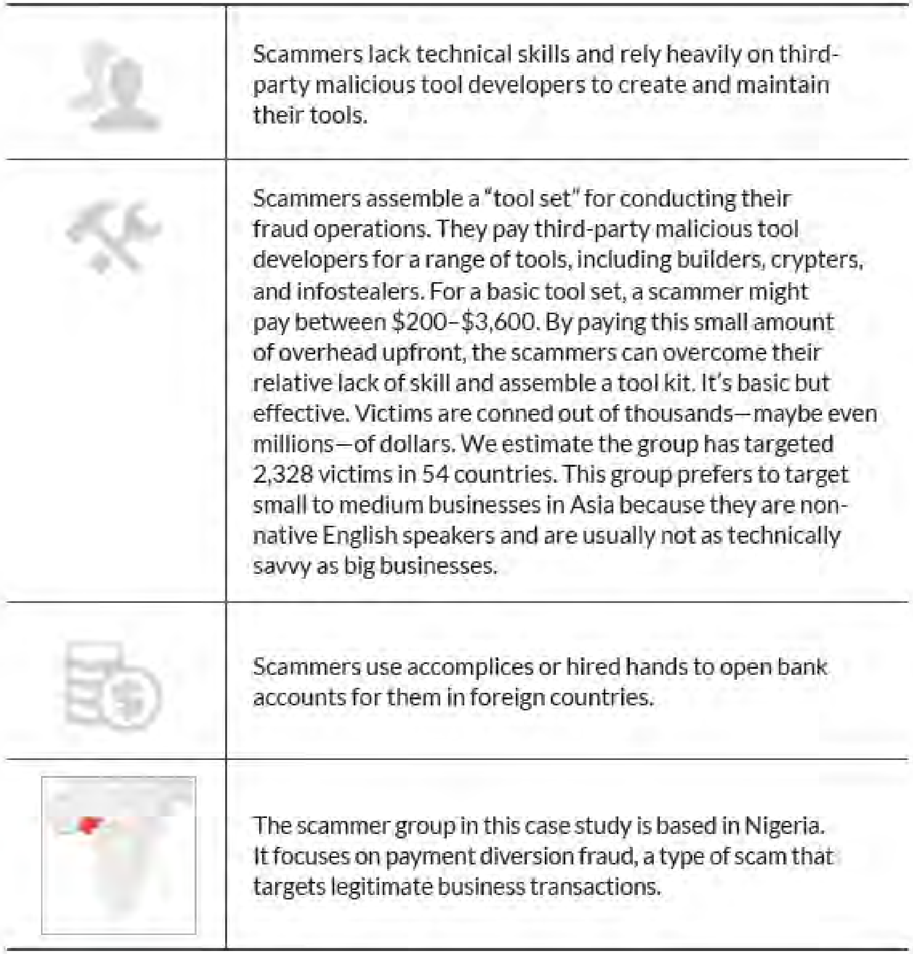
THREAD HIJACKING

-Create visually similar email accounts
-Use malware to steal login information
-Play both sides of transaction

PAYMENT DIVERSION

-Route money to themselves
-Usemules to extract the cash
-Launder the stolen money

Malware – Overview of Nig Group



Scammers lack technical skills and rely heavily on third-party malicious tool developers to create and maintain their tools.

Scammers assemble a "tool set" for conducting their fraud operations. They pay third-party malicious tool developers for a range of tools, including builders, crypters, and infostealers. For a basic tool set, a scammer might pay between $200–$3,600. By paying this small amount of overhead upfront, the scammers can overcome their relative lack of skill and assemble a tool kit. It's basic but effective. Victims are conned out of thousands—maybe even millions—of dollars. We estimate the group has targeted 2,328 victims in 54 countries. This group prefers to target small to medium businesses in Asia because they are non-native English speakers and are usually not as technically savvy as big businesses.

Scammers use accomplices or hired hands to open bank accounts for them in foreign countries.

The scammer group in this case study is based in Nigeria. It focuses on payment diversion fraud, a type of scam that targets legitimate business transactions.

Software Piracy

- Theft of Software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original
  - Examples(Pirate Bay, Bootlegs, etc)
  - End user copying, Downloads

Pedophiles

- Internet allows them to
  - Instant access to other predators worldwide;
  - Open discussion with children
  - Support from other pedophiles
  - Disguise their identities

Pedophiles

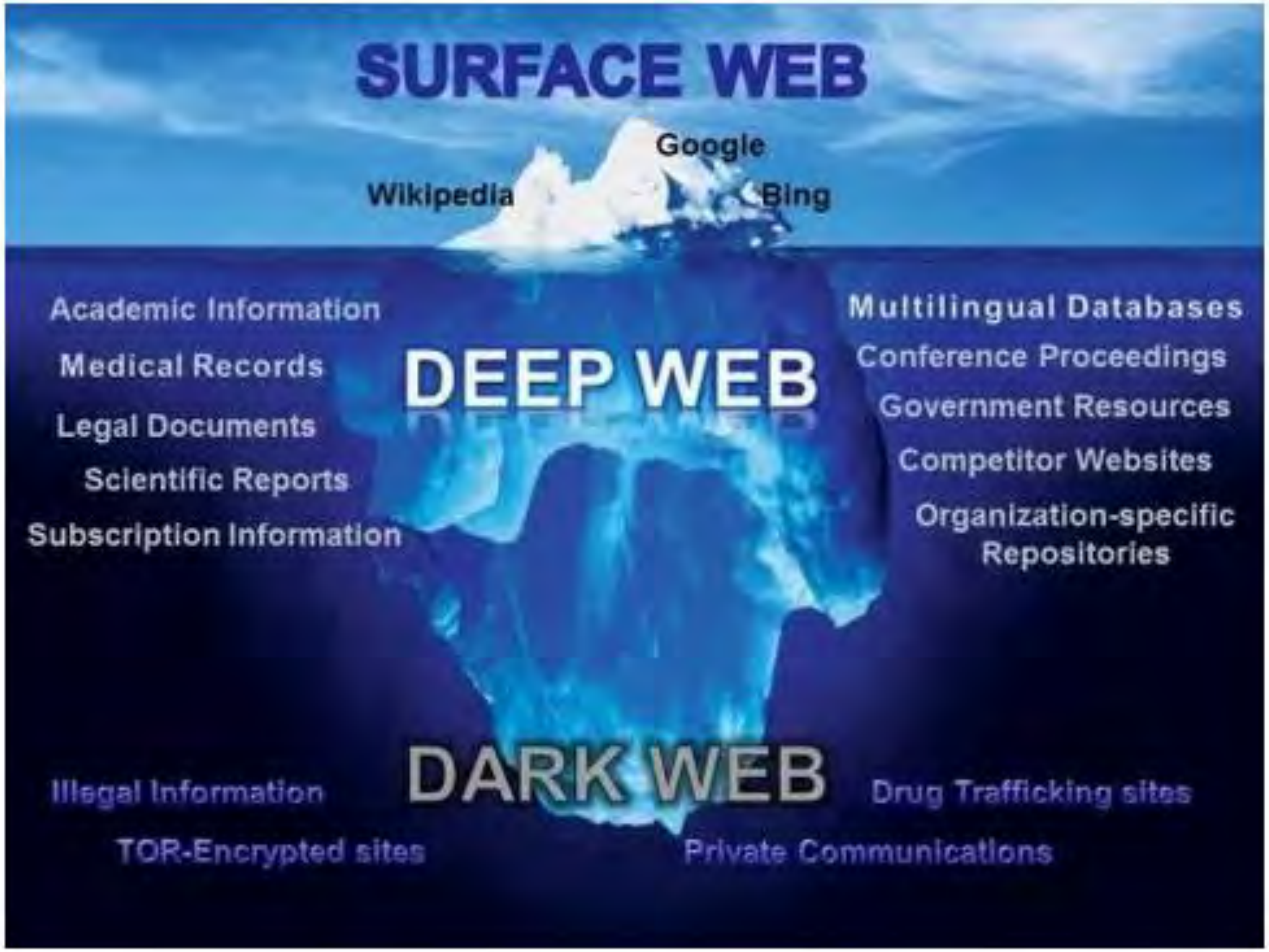
- Pedophile organizations include
- – NAMBLA (The North American Man-Boy Love Association) and
- – PAN (Pedophile Alert Network) in the Netherlands.
- – Members receive monthly magazines and newsletters that include seduction techniques and advice on avoiding detection and prosecution. Pedophiles meet each other via the Internet where they swap methods, success stories, even names, descriptions, and images of children.

IRC Crime

Internet Relay Chat (IRC) servers have chat rooms in which people from anywhere the world can come together and chat with each other

- Criminals use it for meeting coconspirators.
- Hackers use it for discussing their exploits / sharing the techniques
- Pedophiles use chat rooms to allure small children
- Cyber Stalking - In order to harass a woman her telephone number is given to others as if she wants to befriend males

Dark Web


SURFACE WEB
Google
Wikipedia
Bing
Academic Information
Medical Records
Legal Documents
Scientific Reports
Subscription Information
DEEP WEB
Multilingual Databases
Conference Proceedings
Government Resources
Competitor Websites
Organization-specific Repositories
DARK WEB
Illegal Information
TOR-Encrypted sites
Drug Trafficking sites
Private Communications

Dark Web

- ‘Dark web’ is a part of the world wide web that requires special software to access. Once inside, web sites and other services can be accessed through a browser in much the same way as the normal web.
- There are a number of ways to access the dark web (.onion sites), including the use of Tor, Freenet andI2P.

Dark Web – Illegal Contents

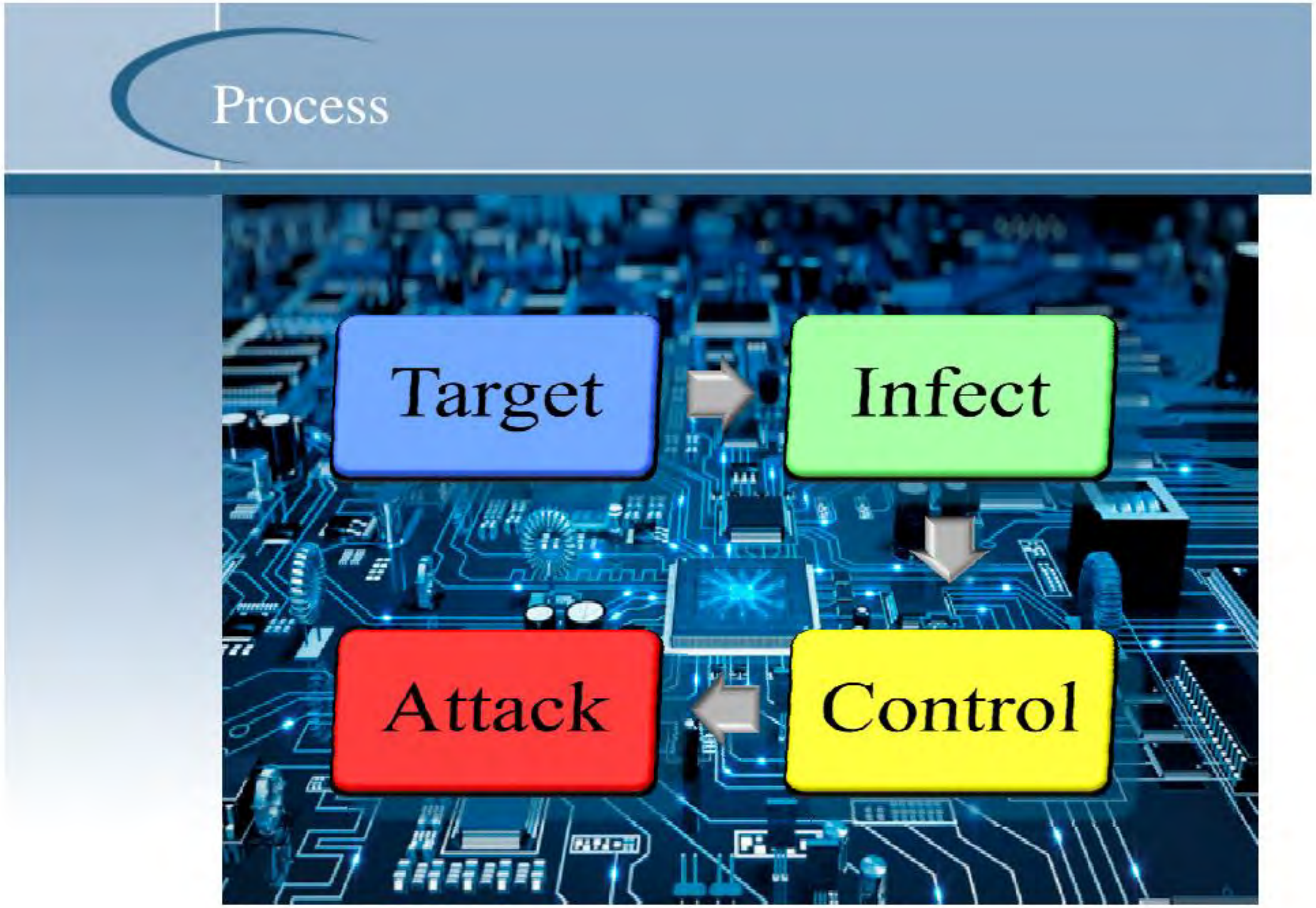
- Pirated music and films
- Drugs and Firearms
- Child pornography
- Credit card details
- Assassination Market
- ETC

- Uses Cryto-currency known as Bitcoin

Social Media

- As social networking becomes more a part of our daily lives, individuals find this technology an attractive vehicle to perpetrate cyber crimes. Anonymity provided via social networks allows a person to easily portray another user's identity. Cyber criminals exploit such vulnerabilities to steal user credentials, which in turn can be used to breach a company's network infrastructure.

Social Media



Process

Target

Infect

Control

Attack

Target

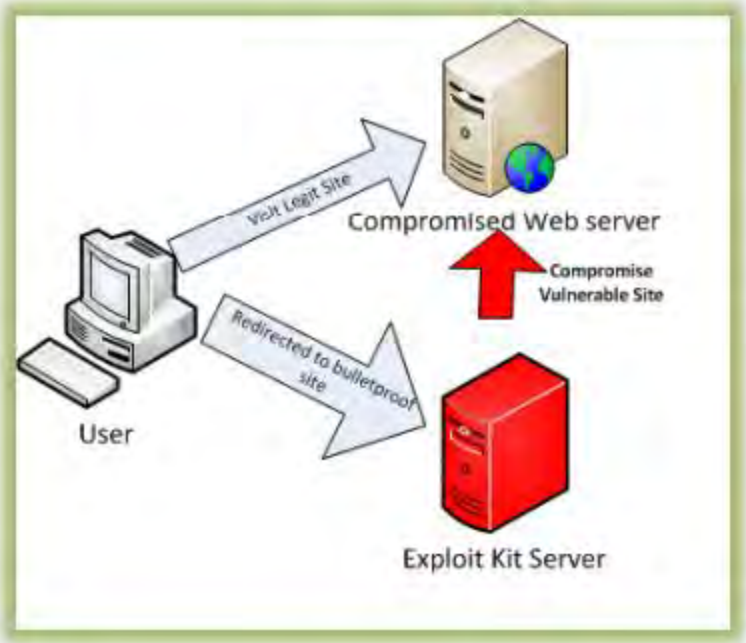
- Cyber criminal communicates with an individual via social media outlet
- Message contains link to fraudulent website or an attachment which initiates an installation file
- Frequently targeted social media networks:
  - – Facebook
  - – Twitter
  - – LinkedIn

Infect

- Cyber attackers use malware payloads to infect a user’s computer or network
    - Types of malware: Trojan Horse, BotNet or Fake AV
- In the past, pop up ads and attachments containing viruses were the primary methods of delivering malware
- Sophisticated techniques now used to compromise legitimate websites in order to spread malware through holes in user’s OS

Web Exploit Kits

- Common Procedure of Web Exploit Kit

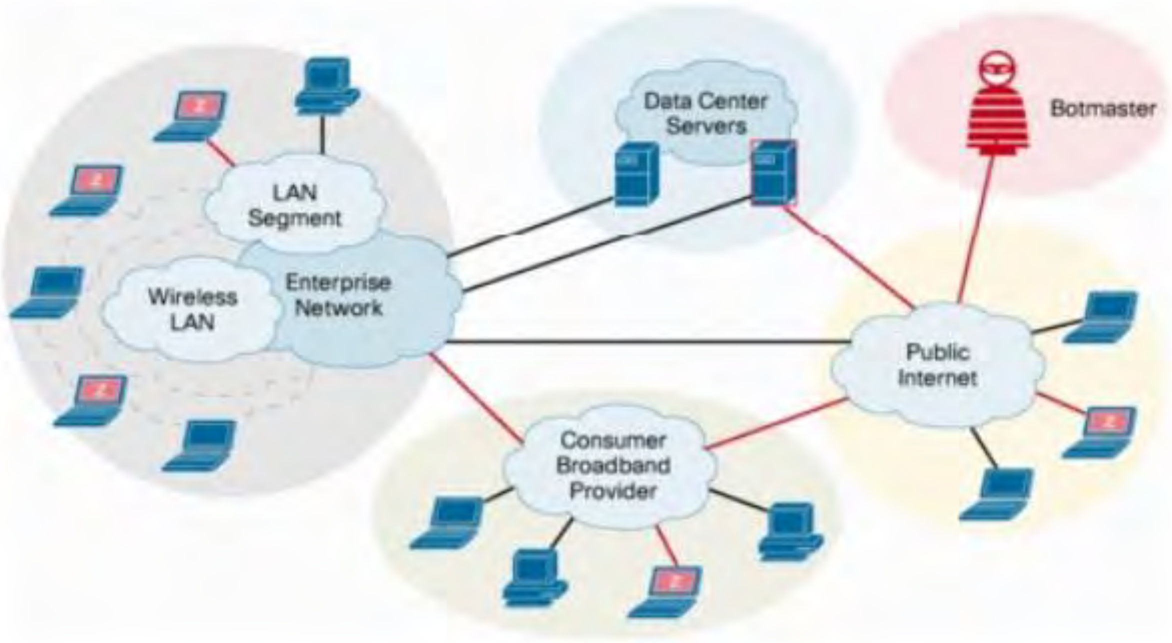


Control

- The infected machine, commonly defined as a “zombie” contacts a public server that the attacker has set up as a control plane to issue commands
- The infected machine will first be controlled to recruit other machines using the same process of scanning for vulnerabilities
- The collection of zombies controlled by one individual is referred to as a BotNet

Botnet

- A typical BotNet with zombies



Attack

- Armed with a network of “zombie” machines, perpetrators can attack on an enormous scale or target specific individual
- Attacks can hypothetically be carried out on any individual, corporate office, government or online retailer connected to the Internet
- Attacks can persist for long duration as proxy connections and IPs are constantly changing by the attacker

Types of BotNet Attacks

- Distributed Denial of Service (DDoS)
- Phishing
- Identity Theft
- Spyware

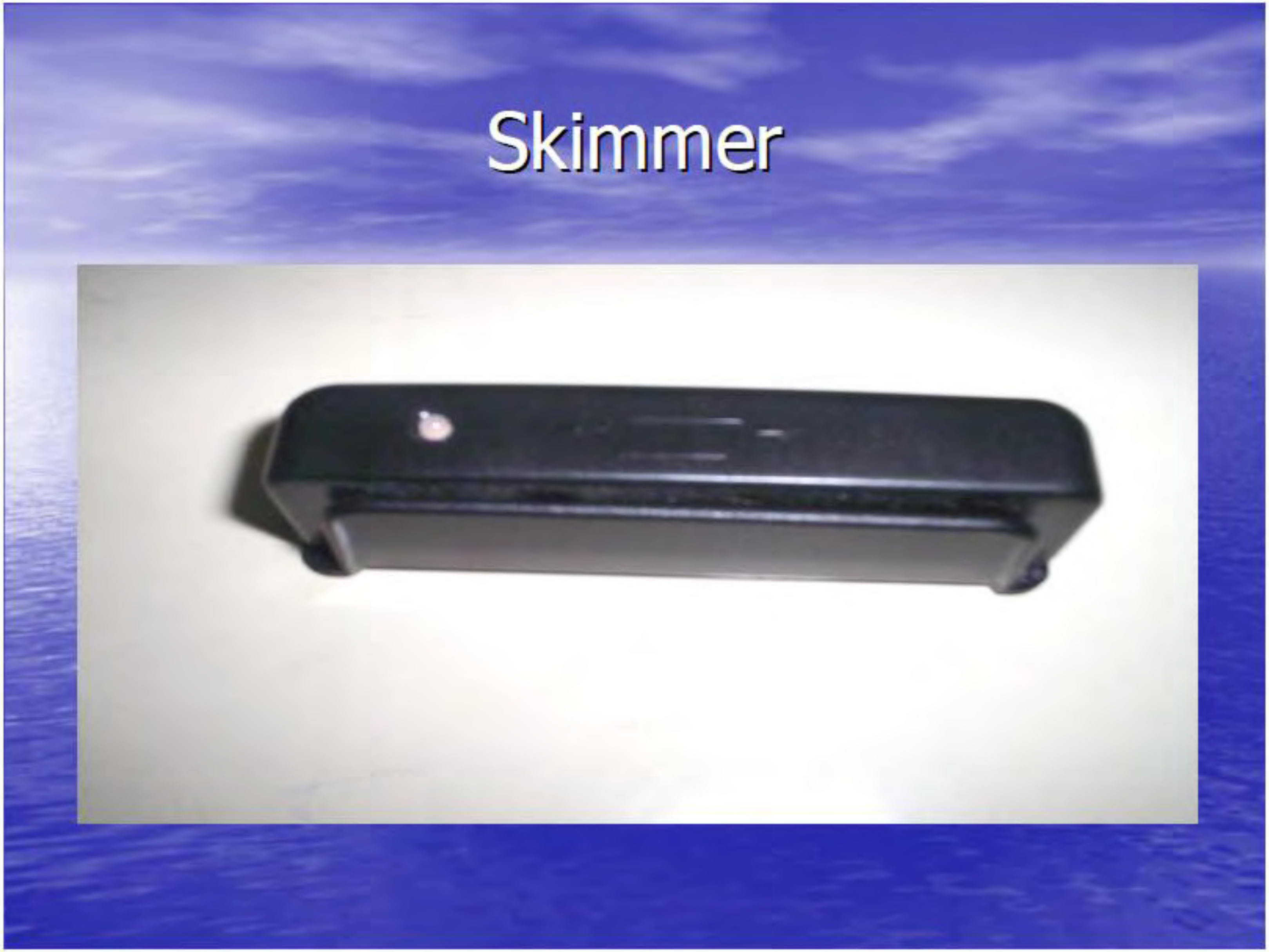
Top 10 Safeguards

- Employee Awareness and Risk Management
- Social Media Privacy Settings
- Access Control
- Vulnerability Management
- Patch Management
- Data Inventory/Protection
- Data Loss Prevention
- Monitor System Configuration Changes
- Leverage Threat Feeds
- Anti-Malware and Anti-Virus Protection

Credit Card Fraud

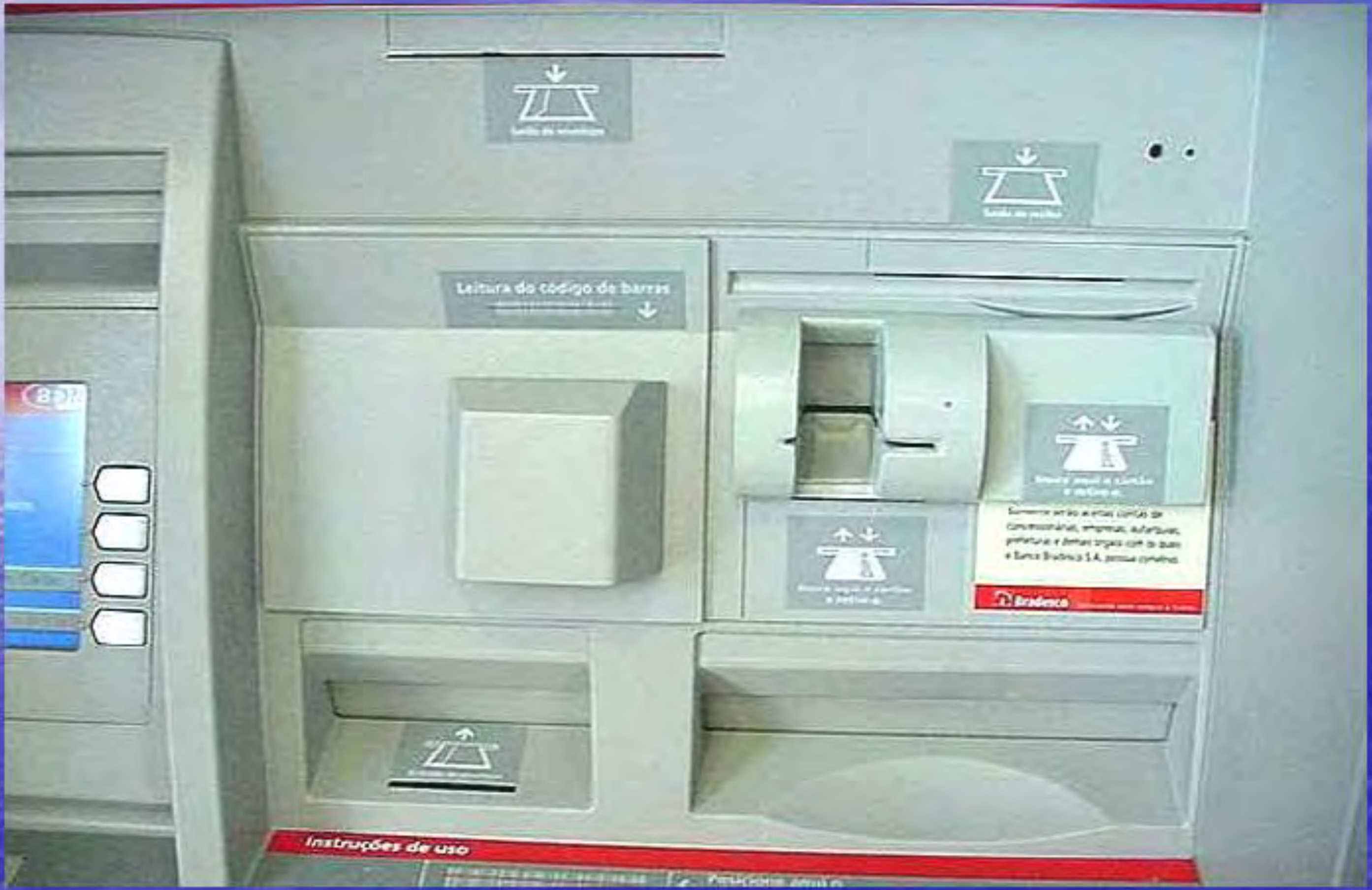
- If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner

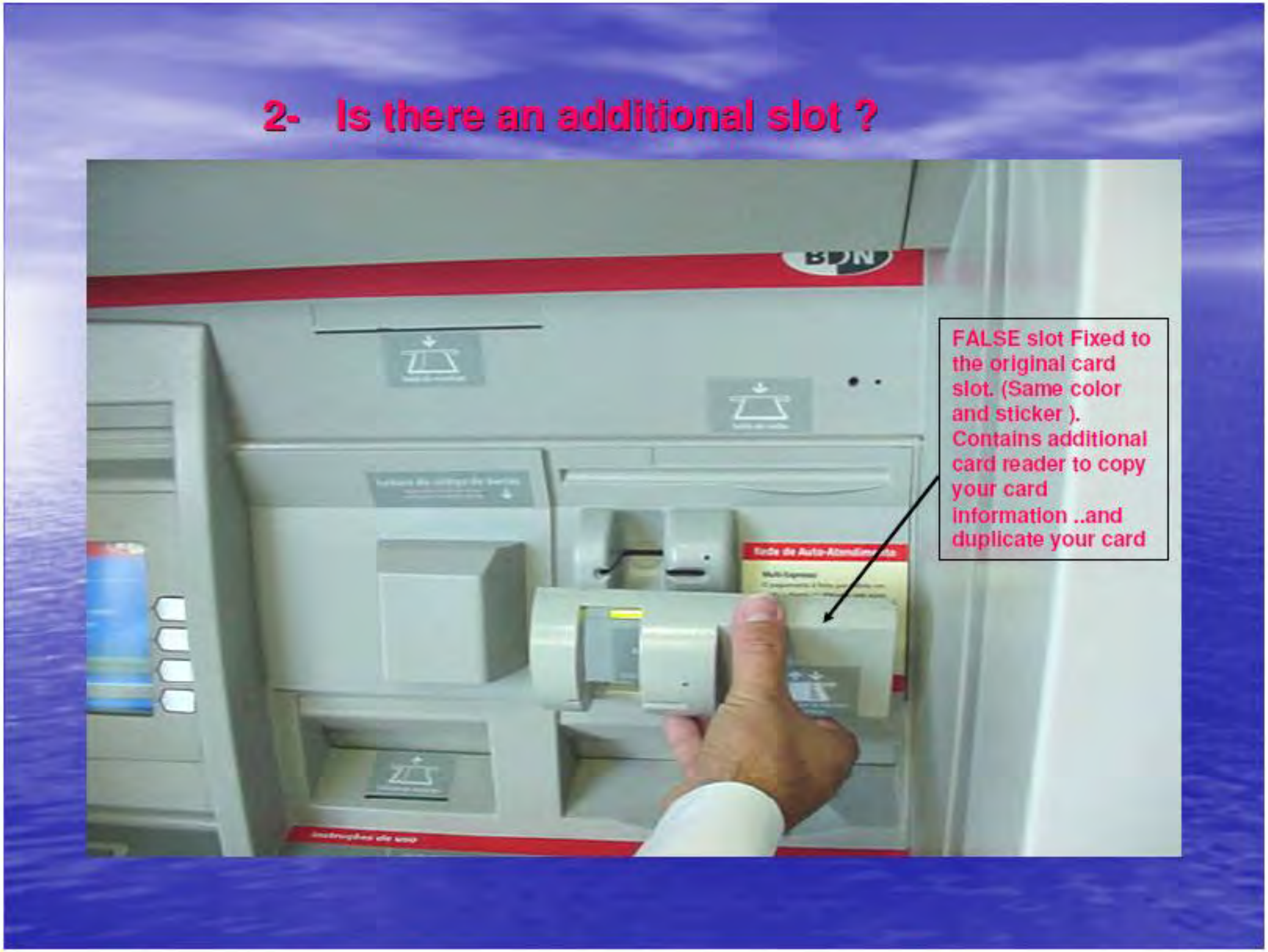
Credit Card Skimmers



Skimmer

1- ATM machine as usual ?

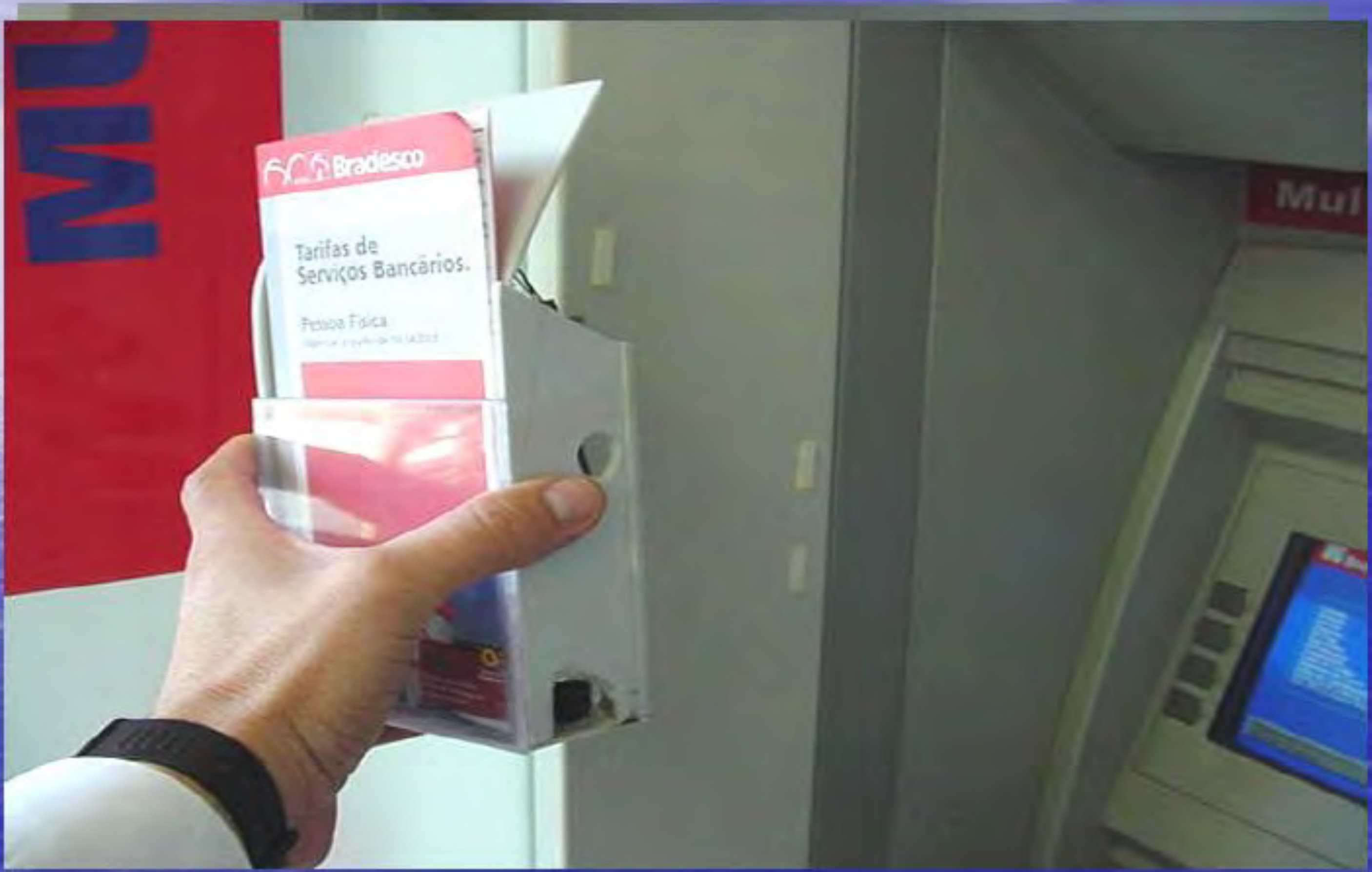




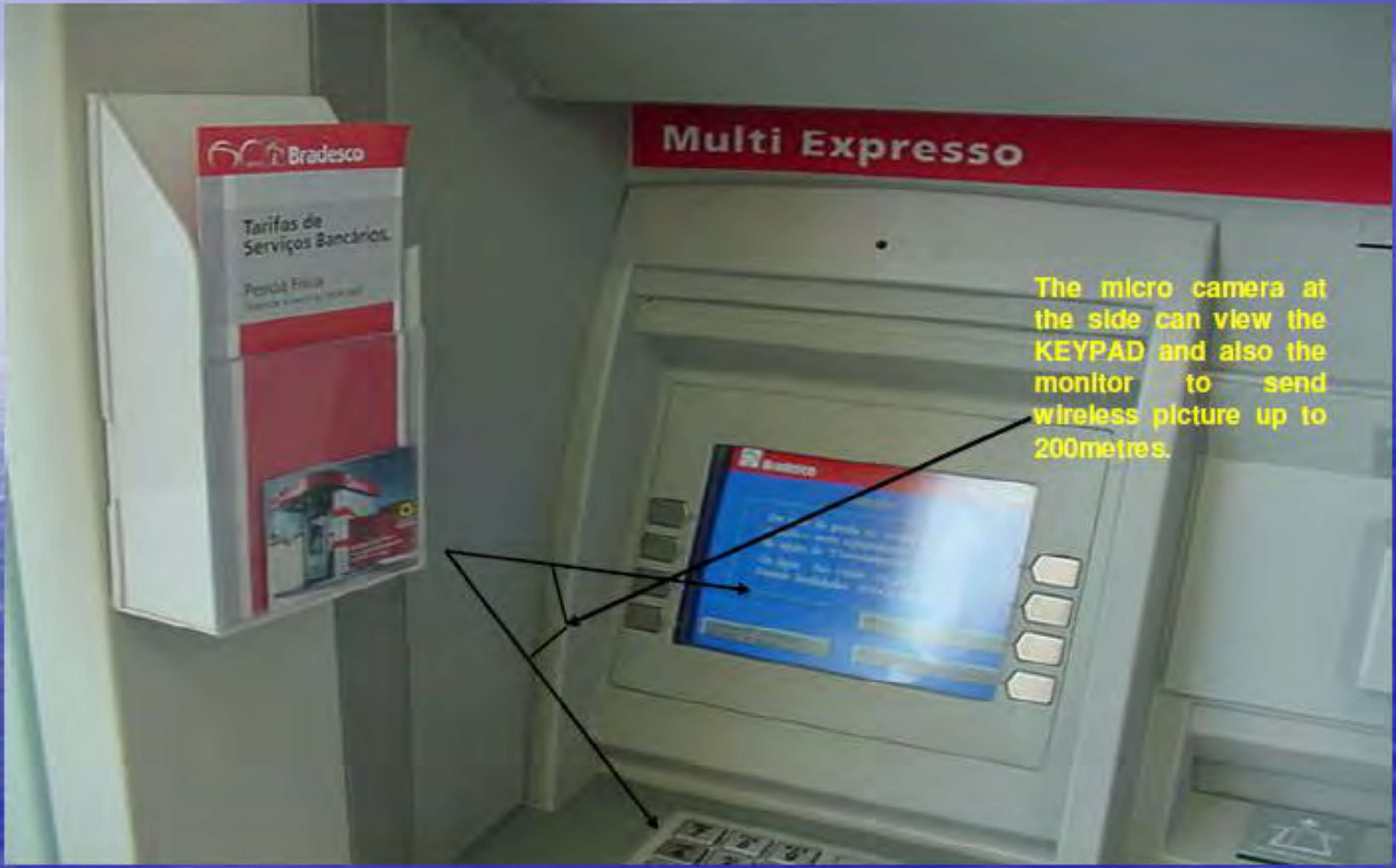
2- Is there an additional slot ?

FALSE slot Fixed to the original card slot. (Same color and sticker). Contains additional card reader to copy your card information ..and duplicate your card

3- A monitor and pamphlet holder at the side...nothing wrong



5-False pamphlet box affixed to the ATM cubicle side



The micro camera at the side can view the KEYPAD and also the monitor to send wireless picture up to 200metres.

NET Extortion

- Copying the company's confidential data in order to extort the company for a huge amount

Phishing

- A technique of pulling out confidential information from the bank/financial accounts by deceptive means

Phishing Methodology

- Contact – Blasting emails using software like harvestor or spider
- Packaging
- Maintain contact with demands
- Introduction of malware

EX: of Phishing Email

From: *****Bank [mailto:support@****Bank.com]
Sent: 08 June 2004 03:25
To: India
Subject: Official information from ***** Bank

Dear valued ***** Bank Customer!

For security purposes your account has been randomly chosen for verification. To verify your account information we are asking you to provide us with all the data we are requesting. Otherwise we will not be able to verify your identity and access to your account will be denied. Please click on the link below to get to the bank secure page and verify your account details. Thank you.

https://infinity.*****bank.co.in/Verify.jsp

****** Bank Limited

Spoofing

- Getting one Computer on the network to pretend to have the identity of another computer, usually one with special access privileges, so as to obtain access to the other computers on the network.

Cyber Stalking

- The criminal follows the victim by sending emails, entering the chat rooms as the person being stalked frequently

Cyber Defamation

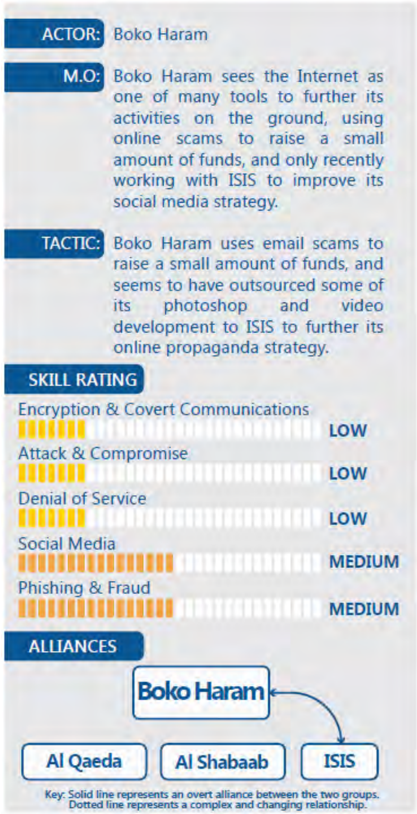
- The Criminal sends emails containing defamatory matters to all concerned off the victim or post the defamatory matters on a website..
- (disgruntled employee may do this against boss,, ex-boys friend against girl,, divorced husband against wife etc)

Threatening

- The criminal sends threatening email or comes in contact in the chat rooms with victim
- (Anyone disgruntled may do this against boss, friend or official)

Terrorism

BOKO HARAM



ACTOR: Boko Haram

M.O: Boko Haram sees the Internet as one of many tools to further its activities on the ground, using online scams to raise a small amount of funds, and only recently working with ISIS to improve its social media strategy.

TACTIC: Boko Haram uses email scams to raise a small amount of funds, and seems to have outsourced some of its photoshop and video development to ISIS to further its online propaganda strategy.

SKILL RATING

Encryption & Covert Communications	LOW
Attack & Compromise	LOW
Denial of Service	LOW
Social Media	MEDIUM
Phishing & Fraud	MEDIUM

ALLIANCES

Key: Solid line represents an overt alliance between the two groups. Dotted line represents a complex and changing relationship.

- Since Boko Haram declared allegiance to ISIS, their propaganda materials have become more sophisticated, suggesting coordination or even that Boko Haram outsources some of its propaganda to ISIS.
- The group has also used online scams, known as 419 scams or letter fraud, as a way to fund its activities.

Salami Attack

- In such crime criminal makes insignificant changes in such a manner that such changes would go unnoticed.
- Criminal makes such program that deducts small amount like Rs. 2.50 per month from the account of all the customer of the Bank and deposit the same in his account. In this case no account holder will approach the bank for such small amount but criminal gains huge amount.

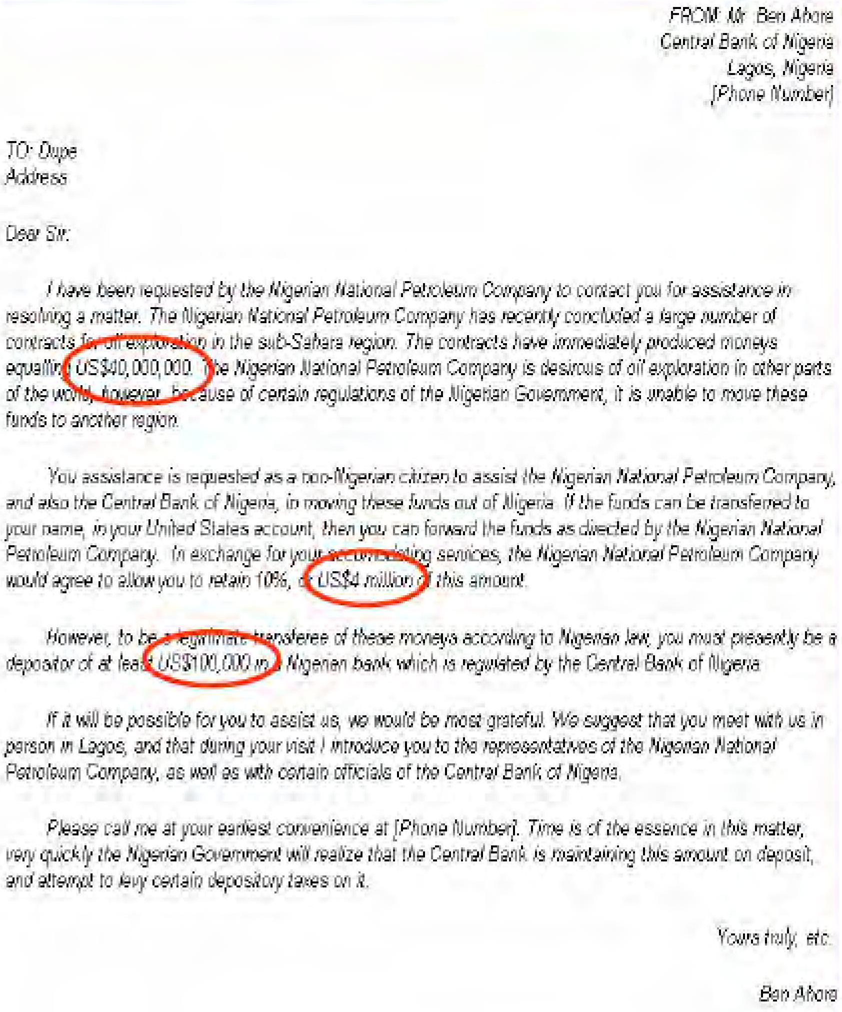
Sale of Narcotics

- Sale and Purchase through the net
- Websites offer sales and shipment of contraband drugs
- May use hidden messages to sell the drugs

Nigeria 4-1-9 Scam

- This scam starts with a bulk mailing or bulk faxing of a bunch of identical letters to businessmen, professionals, and other persons who tend to be of greater-than-average wealth.
- This scam is often referred to as the 4-1-9 scam, ironically after section 4-1-9 of the Nigerian Penal Code which relates to fraudulent schemes

Anatomy of Nigerian Letter



FROM: Mr. Ben Ahore
Central Bank of Nigeria
Lagos, Nigeria
[Phone Number]

TO: Dupe
Address

Dear Sir:

I have been requested by the Nigerian National Petroleum Company to contact you for assistance in resolving a matter. The Nigerian National Petroleum Company has recently concluded a large number of contracts for oil exploration in the sub-Sahara region. The contracts have immediately produced moneys equalling US$40,000,000. The Nigerian National Petroleum Company is desirous of oil exploration in other parts of the world, however, because of certain regulations of the Nigerian Government, it is unable to move these funds to another region.

You assistance is requested as a non-Nigerian citizen to assist the Nigerian National Petroleum Company, and also the Central Bank of Nigeria, in moving these funds out of Nigeria. If the funds can be transferred to your name, in your United States account, then you can forward the funds as directed by the Nigerian National Petroleum Company. In exchange for your accommodating services, the Nigerian National Petroleum Company would agree to allow you to retain 10%, or US$4 million of this amount.

However, to be a legitimate transferee of these moneys according to Nigerian law, you must presently be a depositor of at least US$100,000 in a Nigerian bank which is regulated by the Central Bank of Nigeria.

If it will be possible for you to assist us, we would be most grateful. We suggest that you meet with us in person in Lagos, and that during your visit I introduce you to the representatives of the Nigerian National Petroleum Company, as well as with certain officials of the Central Bank of Nigeria.

Please call me at your earliest convenience at [Phone Number]. Time is of the essence in this matter, very quickly the Nigerian Government will realize that the Central Bank is maintaining this amount on deposit, and attempt to levy certain depository taxes on it.

Yours truly, etc.

Ben Ahore

- My father left me $40 million in his will, but I have to bribe government officials to get it out
- The Nigerian National Petroleum Company has discovered oil, and we as officials of that company want to insider acquire the land, but we need an Indian front man to purchase it first for us
- We just sold a bunch of crude oil in Nigeria, but we have to bribe the banker to get it out
- The Nigerian government overpaid on some contract, and they need a front man to get it out of the country before the government discovers its error

Way forward?

- Criminal Procedural Law
- Electronic Evidence
- International Cooperation
- Liability of Service Provider
- Technical and Procedural Measures
- Under cover work
- Intelligence-led policing
- Capacity Building
- Sharing of Information
- Partnerships with the community, the private sector, and corporations/businesses

Thank you for listening