Cyber Crime

Cyber Theft & Deception

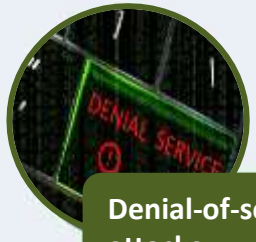
What is Cyber Crime?

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Cybercrime may threaten a person, company or a nation's security and financial health.

Types of cybercrime:

Drug trafficking

Computer viruses
Malware



Denial-of-service attacks

Online harassment

Financial fraud crimes/
Fraud Romance

Cyber-terrorism

Cyber-warfare

Cyber-bullying, Online predator, Cyber-stalking, Cyber Racism, and Internet troll

Cyber-extortion

Obscene or offensive content

What is Cyber Theft?

Cybercrime is one of the most crucial problems faced by the countries across the globe these days. It includes unauthorized access of information and break security like privacy, password, etc. of any person with the use of internet. Cyber theft is a part of cybercrime which means theft carried out by means of computers or the Internet. Cyber theft is when your financial or personal information is stolen via computers.

Types of Cyber Theft:

Identity Theft 01

Identity theft pertains to illegally obtaining of someone's personal information which defines one's identity for economic benefit. Identity theft pertains to illegally obtaining of someone's personal information which defines one's identity for economic benefit.

Financial fraud 02

Any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. Forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information.

Internet time theft 03

It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person. The authorized person gets access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.

Intellectual Property Theft 04

Intellectual property (IP) theft is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations etc. One of the most commonly and dangerously known consequence of IP theft is counterfeit goods and piracy.

What is Cyber Identity Theft?

Cyber identity theft refers to the on-line misappropriation of identity tokens using information and communication technologies.

Who are the victim?

Identity theft can take place whether the fraud victim is alive or deceased. Creating a fake account or impersonation by creating multiple email-ids has become quite common and has resulted in commission of fraud in order to obtain any such information which can be used by cyber criminals to take over the victim's identity to commit myriad crimes. The advancement of technology has made things much easier as it is much difficult to track the person impersonating as Internet and online transactions provides a kind of anonymity and privacy to an individual.

The crime of identity theft consists of two steps:

✓ Wrongful collection of personal identity of an individual

✓ Wrongful use of such information with an intention of causing legal harm to that person information

How does identity theft happen?

Hacking

Cybercriminals often hack the computer of the victim and then control the activities of the victim. Hacking refers to the authorized access to someone's computer.

Phishing

It uses fake email-ids/ messages containing viruses affected websites. These infected websites urge people to enter their personal information such as login information, account's information.

E-Mail/SMS Spoofing

The spoofed e-mail is one which shows its origin to be different from where it actually originated. In SMS spoofing, the offender steals identity of another person in the form of phone number.

Pharming

Cybercriminal installs a malicious code on the personal computer or server misdirecting users to a fraudulent website without their consent or knowledge. Pharming disguises fake, fraud, data grabbing website.

Credit Card Skimming

The victims of credit card sk imming find fraudulent withd rawal of money and charge s on their account. It is surpr ising to note that all this hap pens to the victim is in poss ession of the credit card.

Malicious software

Software designed to harm the victim's computer. Malware is installed on he victim's comput er without his consent. The us er is directed to move on to a malicious site by clicking on a malicious link.

What is Financial Fraud Crime?

Significantly, this crime was one simultaneous, coordinated attack against many banks. They also made use of several channels, including ATMs, credit and debit cards, and wire transfers.

World Economic Forum noted that fraud and financial crime was a trillion-dollar industry, reporting that private companies spent approximately $8.2 billion on anti–money laundering (AML) controls alone in 2017..

***The incidents of online financial fraud outnumbered others by a big margin and a major contributor to this is the lack of due diligence or carelessness on the part of the victims. Led by financial fraud, cyber crime touched peak in lockdown months*.**

Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. Altering or deleting stored data. These types of crime often result in the loss of private information or monetary information.

Altering in an unauthorized way. This requires little technical expertise and is a common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes.

.

The new cyber profile of fraud and financial crime is well illustrated by the Carbanak attacks.

1. Spear phishing
Employee in targeted organization receives email with the Carbanak backdoor as an attachment

2. Backdoor executed: credentials stolen
Upon opening attachment, employee activates the Carbanak backdoor

3. Machines infected in search for admin PC
Carbanak searches network and finds admin PC; embeds and records

4. Admin PC identified, clerk screens intercepted
Attacker watches admin screen to mimic admin behavior for the bank's cash-transfer systems

5. Balances inflated and inflated amount transferred
Attackers alter balances, pocket extra funds ($1k account enlarged to $10k, then $9k transferred)

6. ATM programmed to dispense cash
Attackers program ATMs to issue cash to waiting accomplices at specific times

7. Cash moved through channels by wire transfers, e-payments
Attackers use online and e-payments to receiver banks to transfer extracted funds

Crime pathways are converging, blurring traditional distinctions among cyber breaches, fraud, and financial crimes.

Fraud and insider threats

- Internal and external threats
- Retail and nonretail threats
- Insider threats
- Market abuse and misbehavior

Cyber breaches

- Confidentiality
- Integrity
- Systems availability

Financial crimes

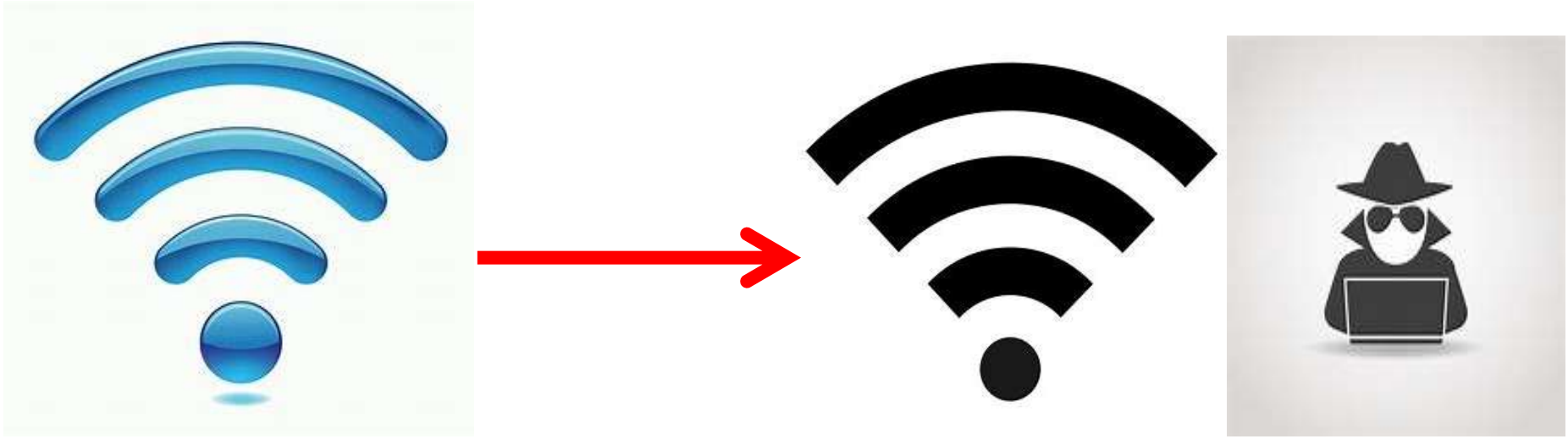
- Money laundering
- Bribery and corruption
- Tax evasion and tax fraud

Example: cyberattack on a central bank

- Bank employee's SWIFT[1] credentials stolen with the help of insiders
- Malware surreptitiously installed on the bank's computers to prevent discovery of withdrawals
- Funds routed from bank's account at a branch of another country's central bank to a third bank (on a weekend to ensure staff absence)
- Withdrawals were made at the third bank through multiple transactions that were not blocked until too late
- Attacks may have been linked to a known sanctioned entity

What is Internet Time Theft?

It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person. The authorized person gets access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.



What is Theft of Intellectual Property?

Intellectual property (IP) theft is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations etc. One of the most commonly and dangerously known consequence of IP theft is counterfeit goods and piracy.

Cyber Deception Technology

With traditional cyber security, companies play a cat-and-mouse game to identify, block, and prevent threats. A deception program changes this by giving defenders the ability to learn about attackers in the same way attackers try to learn about their targets. Once an organization knows an attacker is in the network, it can observe the attacker's behaviors and patterns. This background helps security teams better understand what attackers are after and the best way to respond.

Today's cyber operations have been designed to respond only after attacks take place. Cyber deception is an emerging proactive cyber defense methodology that, when done well, can put the defender in the driver's seat. It enables defenders to lead the attacker and gather intelligence on the adversary's tools, methods, and behaviors. In this way, defenders have the upper hand in cyber operations.

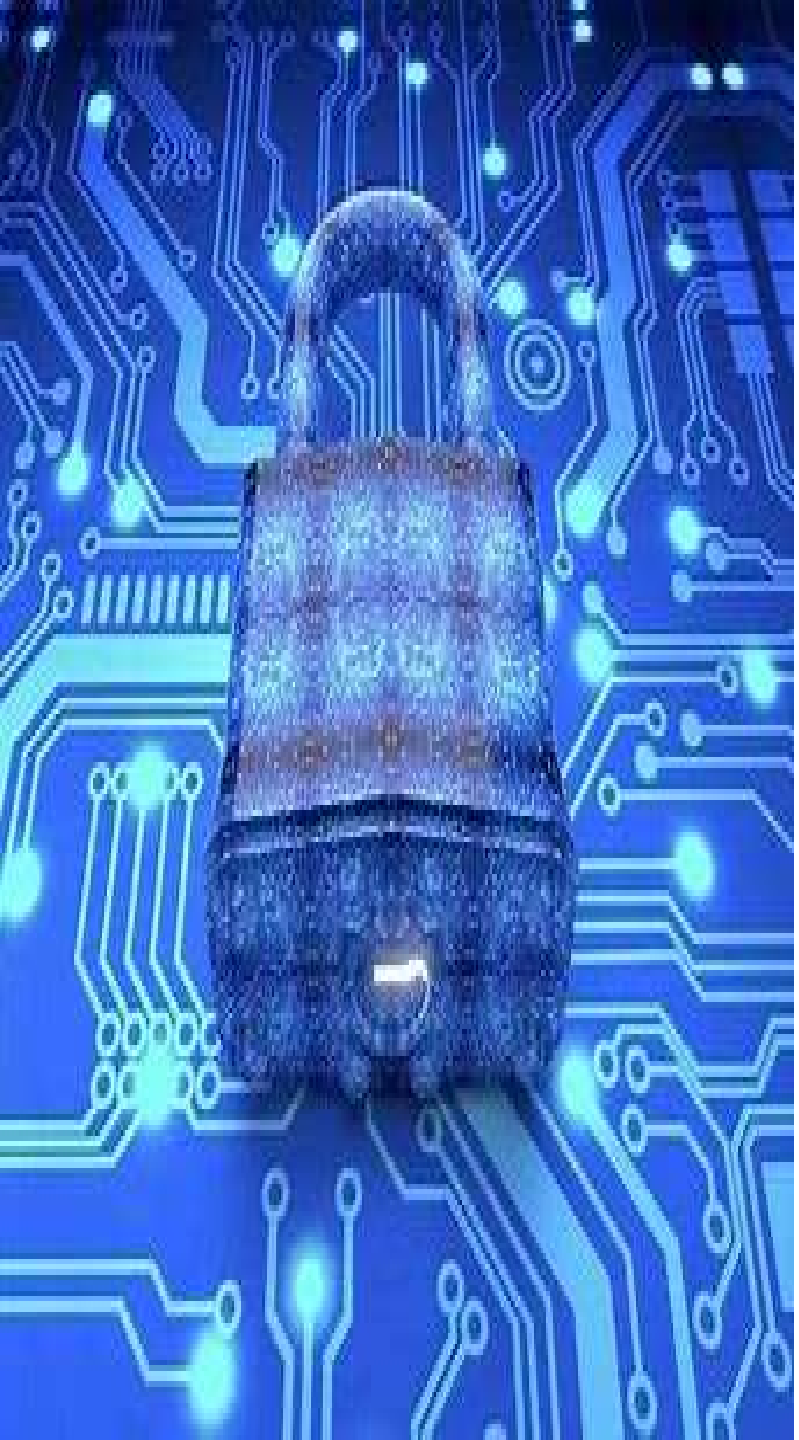
Earlier Technology Used for Cyber Security- Honeypots

Honeypot Technology

In computer terminology, a honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site that seems to contain information or a resource of value to attackers, but actually, is isolated and monitored and enables blocking or analyzing the attackers. This is similar to police sting operations, colloquially known as "baiting" a suspect.

Deception Technology

Recently, a new market segment called deception technology has emerged using basic honeypot technology with the addition of advanced automation for scale. Deception technology addresses the automated deployment of honeypot resources over a large commercial enterprise or government institution. The technology works by generating traps or deception decoys that mimic legitimate technology assets throughout the infrastructure.



Deception Technology

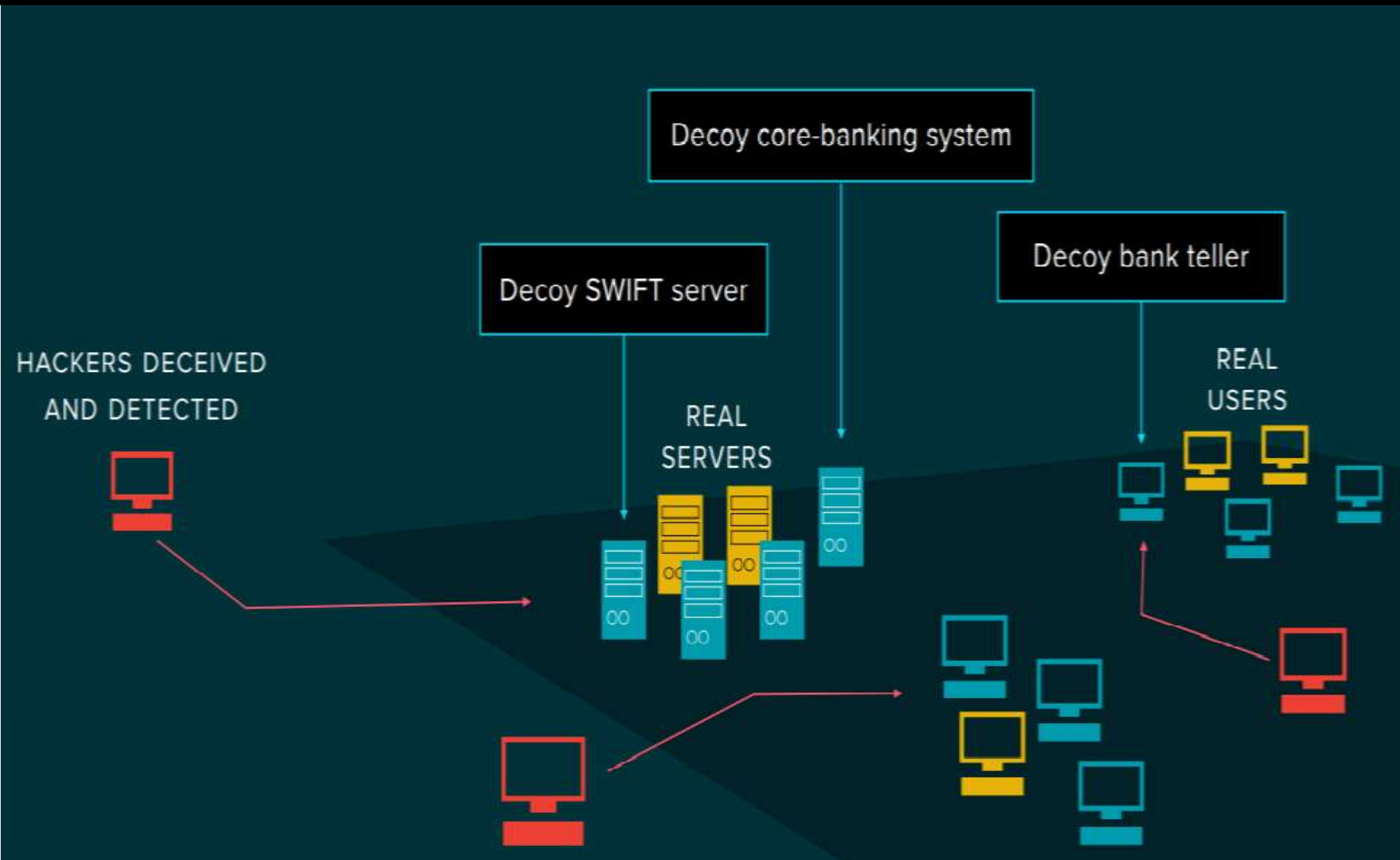
is an evolved form of cybersecurity which aims to turn the current paradigm on its head – from reactionary to proactive defense.

The aim of deception technology is to prevent a cybercriminal that has managed to infiltrate a network from doing any significant damage. The technology works by generating traps or deception decoys that mimic legitimate technology assets throughout the infrastructure. These decoys can run in a virtual or real operating system environment and are designed to trick the cybercriminal into thinking they have discovered a way to escalate privileges and steal credentials. Once a trap is triggered, notifications are broadcast to a centralized deception server that records the affected decoy and the attack vectors that were used by the cybercriminal.

Why Use Deception Technology?

Deception Technology can provide a low-cost, efficient method of determining if an internal or external breach is in process. When deception technology that has been implemented correctly detects an alert, you can be assured that false positives have been eliminated and the alert is real. These technologies can surveillance a threat actor while they are going about their business and capture those interactions for enhanced defenses and threat intelligence. This threat intelligence can help an organization understand who is targeting them and how by gathering the tactics, techniques, and procedures (TTPs) of an attacker. For a MSSP, like One Source, it allows us to build out rules and protections for our clients from real and current data. These high-quality alerts allow organizations to enhance their prevention and defenses more effectively.

Deception surrounds **banking systems with decoys** that detect hackers before any business impact



The advantages of Cyber Deception Technology:

It is an overlay approach to cyber security that can change the way many organisations work to prevent data breaches, malicious code and denial- of- service attacks. This will force attackers into a world of unreliable data that renders attacks useless.

1. Detect all high-risk threats
2. Complete visibility
3. Low false positives
4. Real-time detection
5. Covers the entire kill-chain

Research and Presentation by:

Name- Ananya Ghosh

Reg. No.- 20MIC0063

Slot: C1

Event: Seminar on Module 7 topics