Cybersecurity : Threats & Solutions

Industry Perspective.

It begins.

- “The only system which is truly secure is one which is switched off and unplugged, locked in a titanium safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn’t stake my life on it.”

Professor Gene Spafford

Cyber Security : Definition

- Cyber security is the body of technologies, processes and practices involved in protecting individuals and organizations from cyber crime and now cyber warfare.
- It is designed to protect integrity of networks, computers, programs and data from attack, damage or unauthorized access
- There are five key principles in cyber security:
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
  - Auditability

More popular triad of Cybersecurity.

Scope of Cybersecurity.

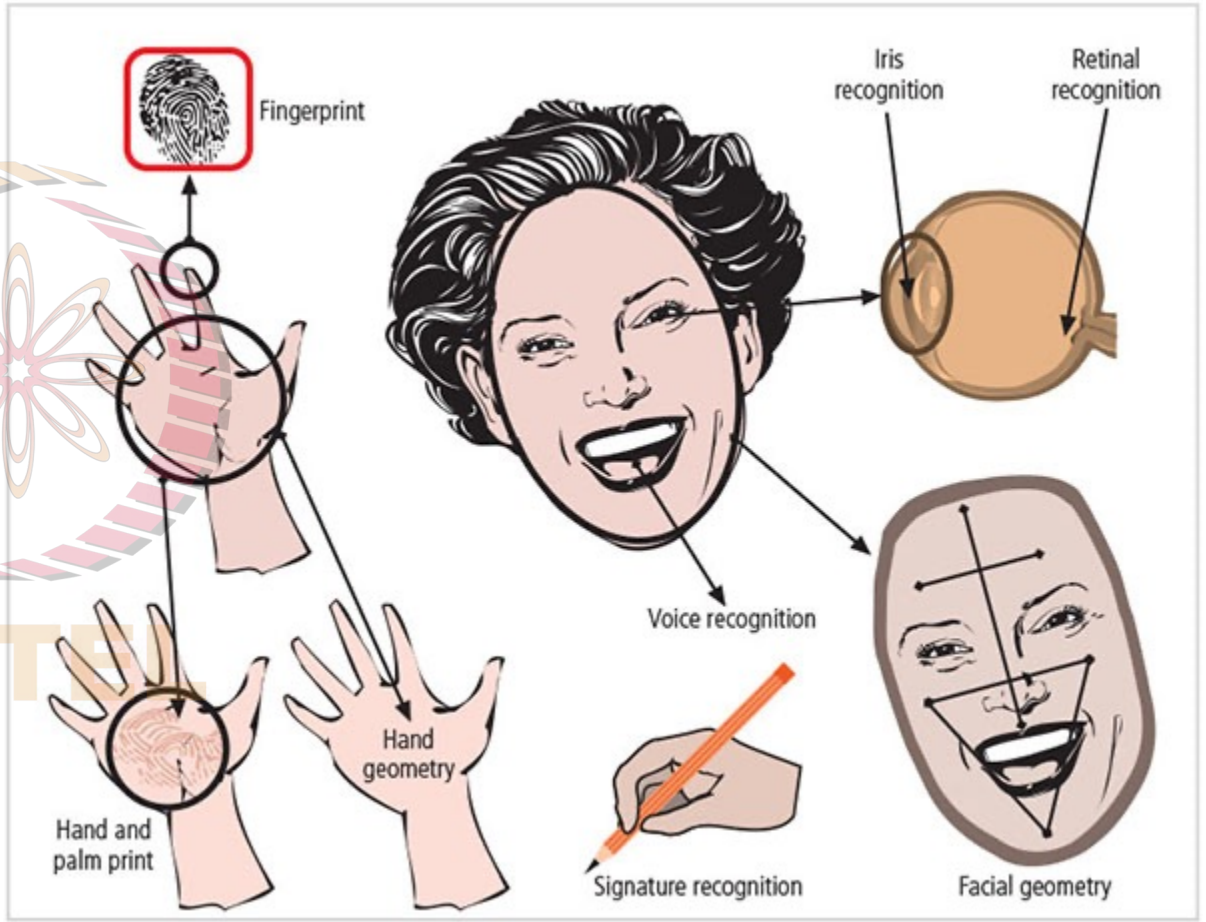
First Cyber attack (1982) !

Take the dubious story of a Soviet pipeline explosion back in 1982, much cited by cyberwar's true believers as the most destructive cyberattack ever. The account goes like this: In June 1982, a Siberian pipeline that the CIA had virtually booby-trapped with a so-called "logic bomb" exploded in a monumental fireball that could be seen from space. The U.S. Air Force estimated the explosion at 3 kilotons, equivalent to a small nuclear device. Targeting a Soviet pipeline linking gas fields in Siberia to European markets, the operation sabotaged the pipeline's control systems with software from a Canadian firm that the CIA had doctored with malicious code. No one died, according to Thomas Reed, a U.S. National Security Council aide at the time who revealed the incident in his 2004 book, *At the Abyss*; the only harm came to the Soviet economy.

But did it really happen? After Reed's account came out, Vasily Pchelintsev, a former KGB head of the Tyumen region, where the alleged explosion supposedly took place, denied the story. There are also no media reports from 1982 that confirm such an explosion, though accidents and pipeline explosions in the Soviet Union were regularly reported in the early 1980s. Something likely did happen, but Reed's book is the only public mention of the incident and his account relied on a single document. Even after the CIA declassified a redacted version of Reed's source, a note on the so-called Farewell Dossier that describes the effort to provide the Soviet Union with defective technology, the agency did not confirm that such an explosion occurred. The available evidence on the Siberian pipeline blast is so thin that it shouldn't be counted as a proven case of a successful cyberattack.

Concepts of Cyber Security

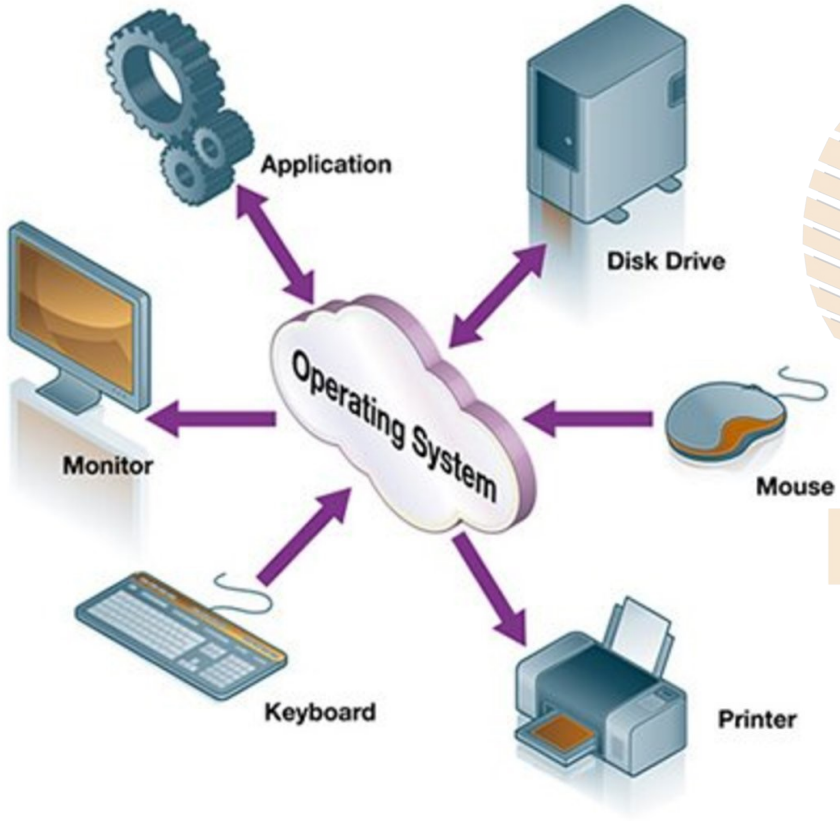
Basics to Intermediate users.

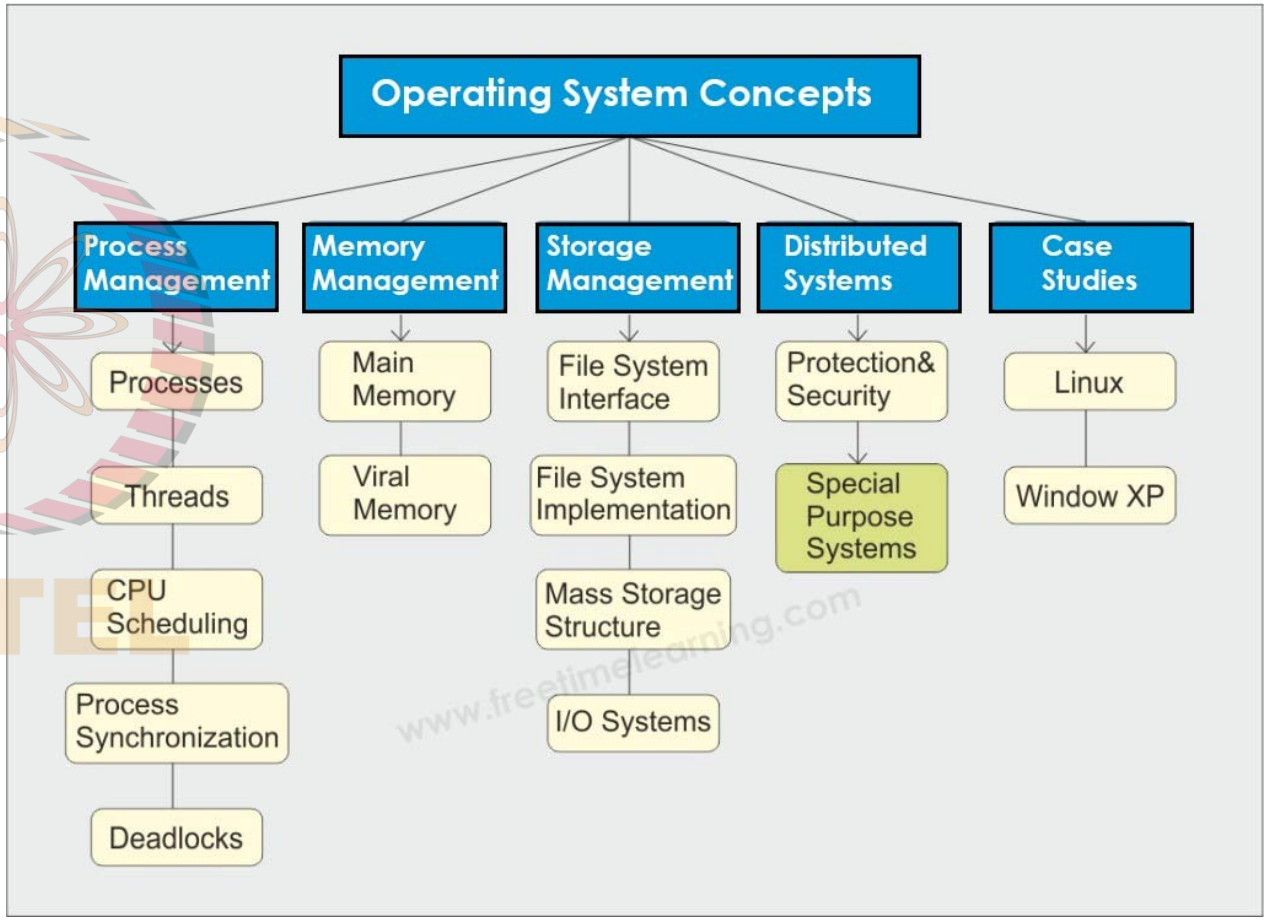


Introduction to Concepts : Cyber Security

- **General Concepts**
  - Operating Systems
  - Cryptography
- Networking Concepts
  - OSI Model
  - Packets & Protocols
  - Firewalls
  - Design of a Simple Network
  - Connecting to Network
- Security Concepts
  - CIA Triad
  - Cyber Operational Concepts & Terms.
- Workshop & Discussion
  - QBOT : Execution
  - QBOT : Analysis

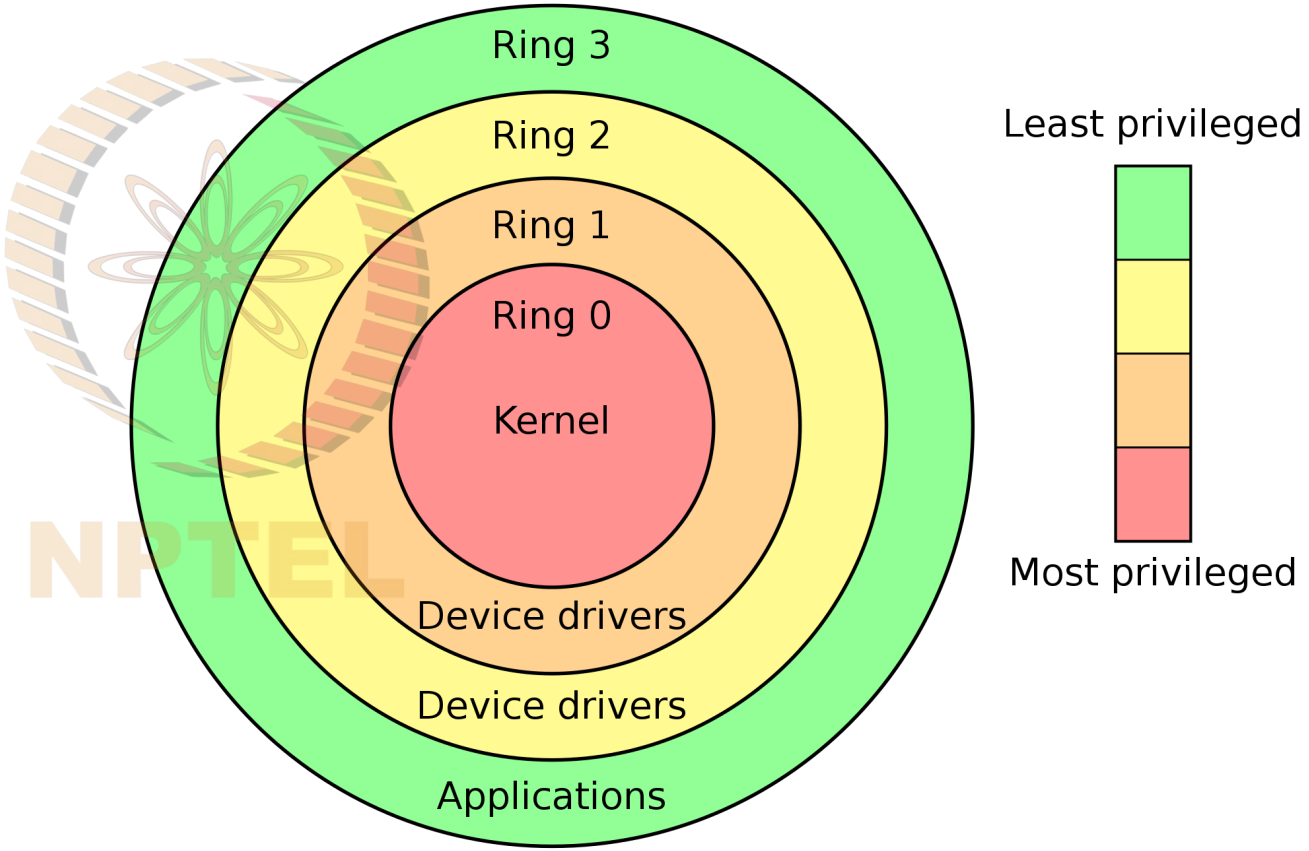
Operating Systems.



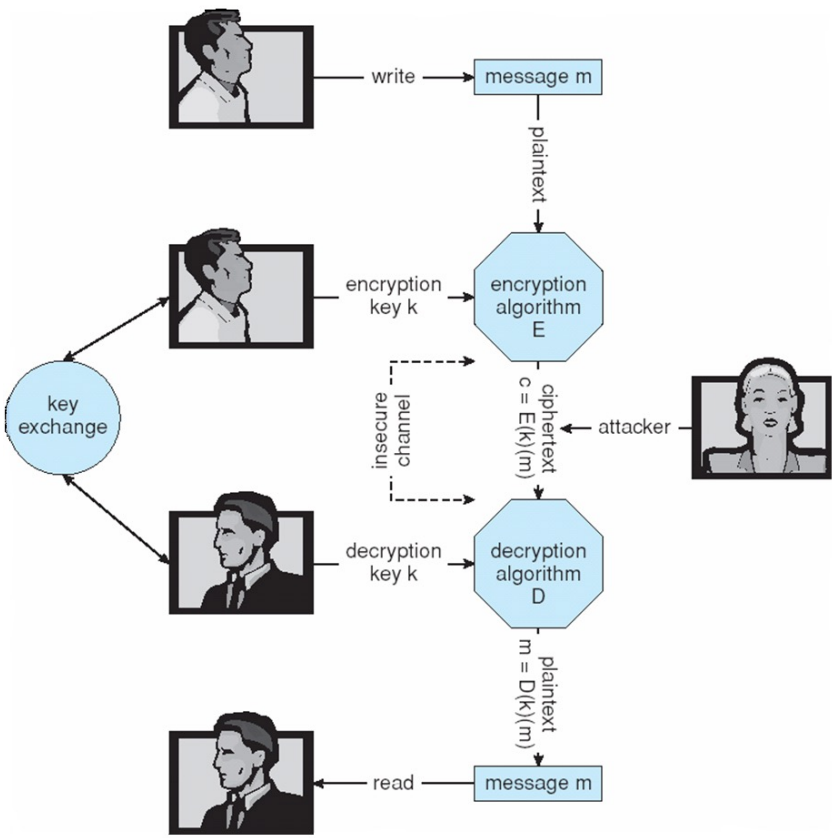


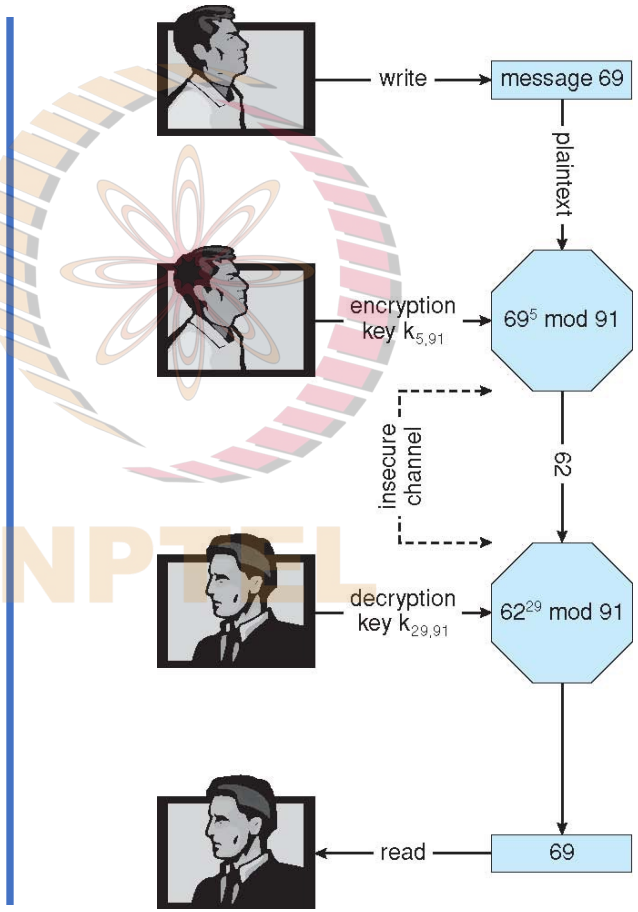
Rings for all.

Operating System has multi-layered defense systems internally enforced.

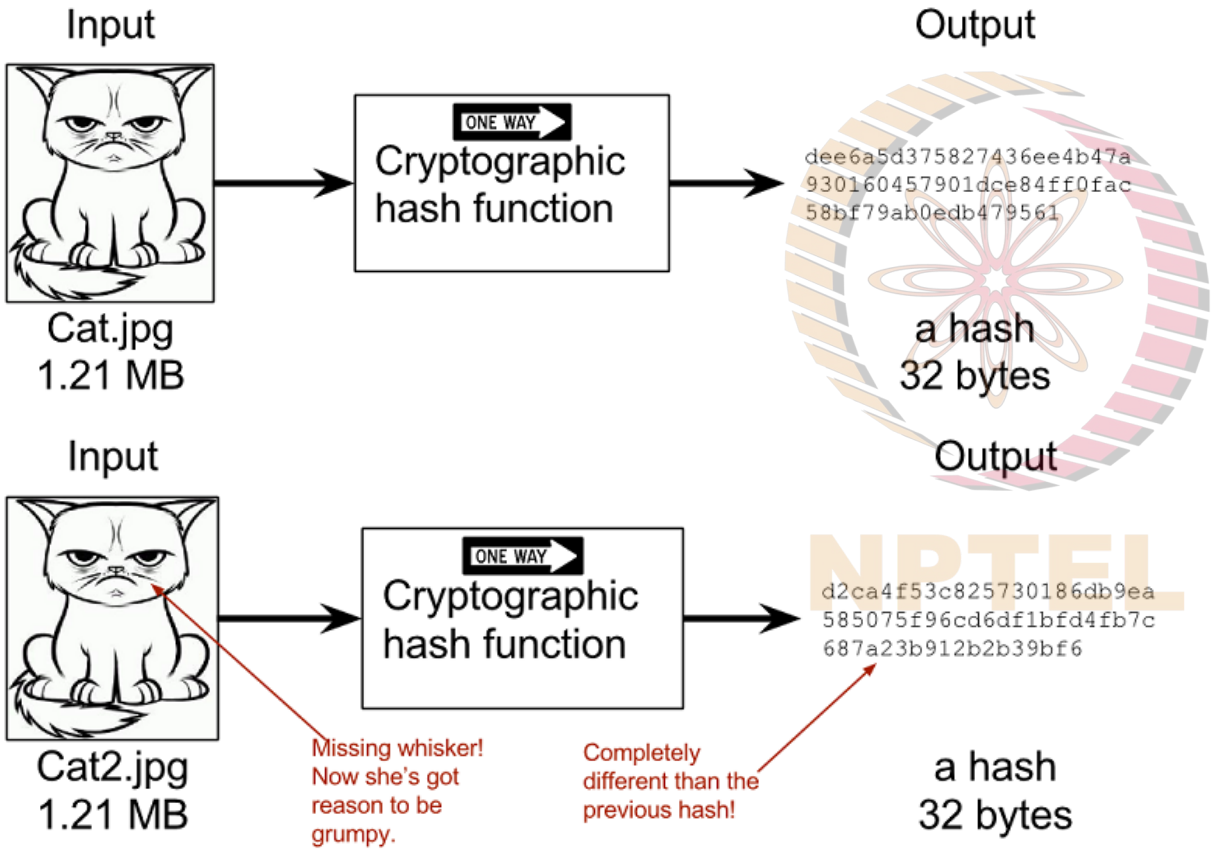


Cryptography: PKI Basics.

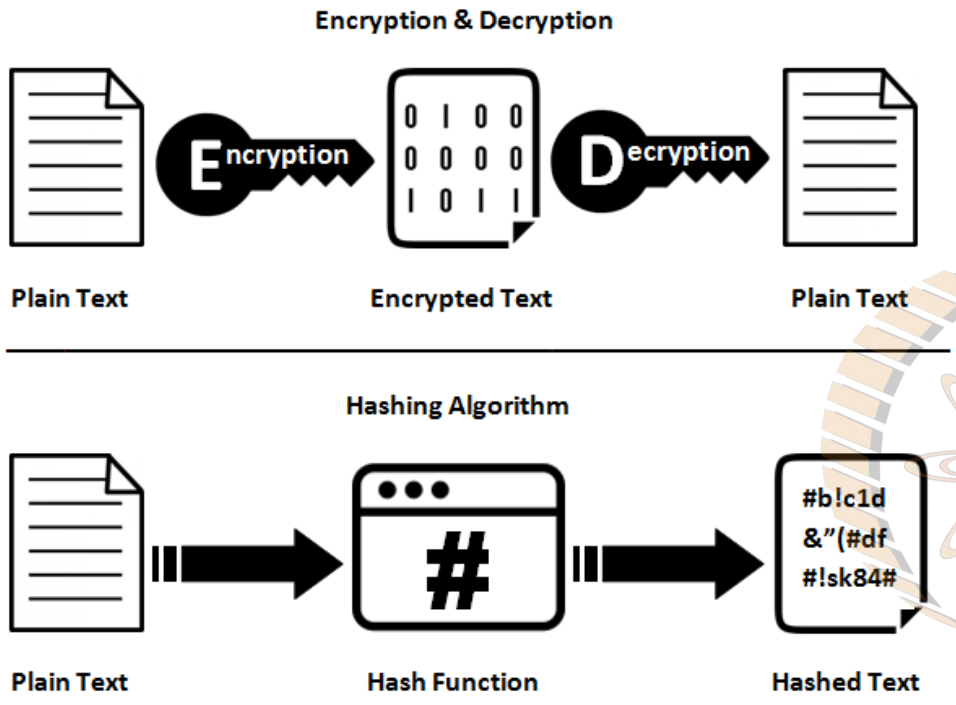


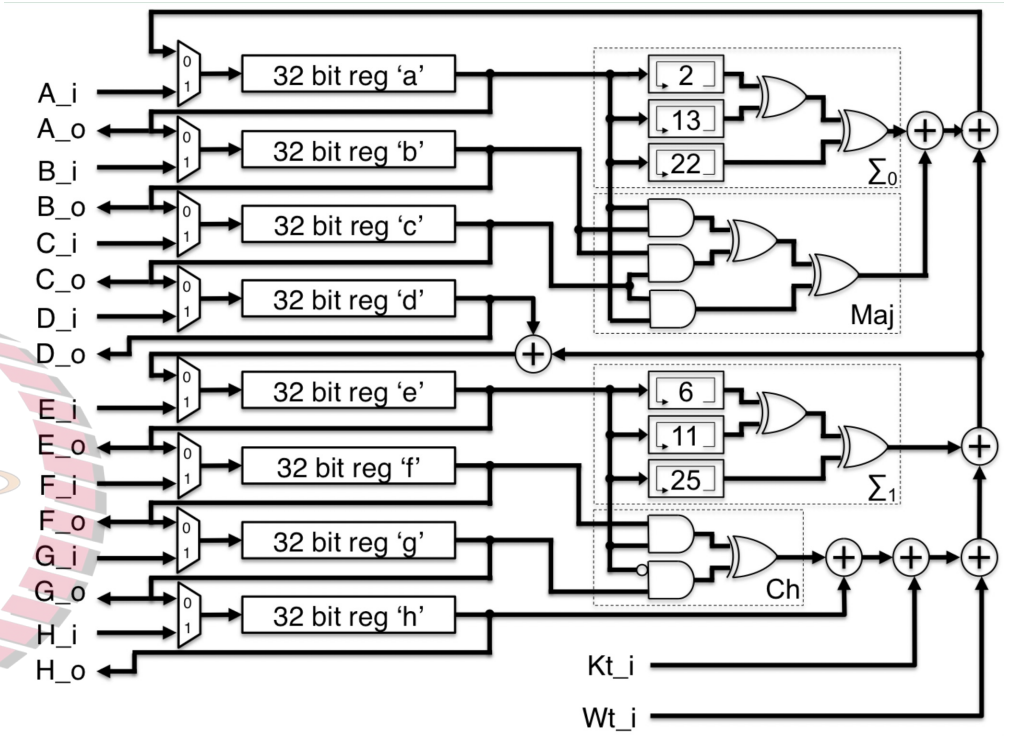


Cryptography : Hash function.



- One sided computation is fast.
- Reversing is nearly impossible.



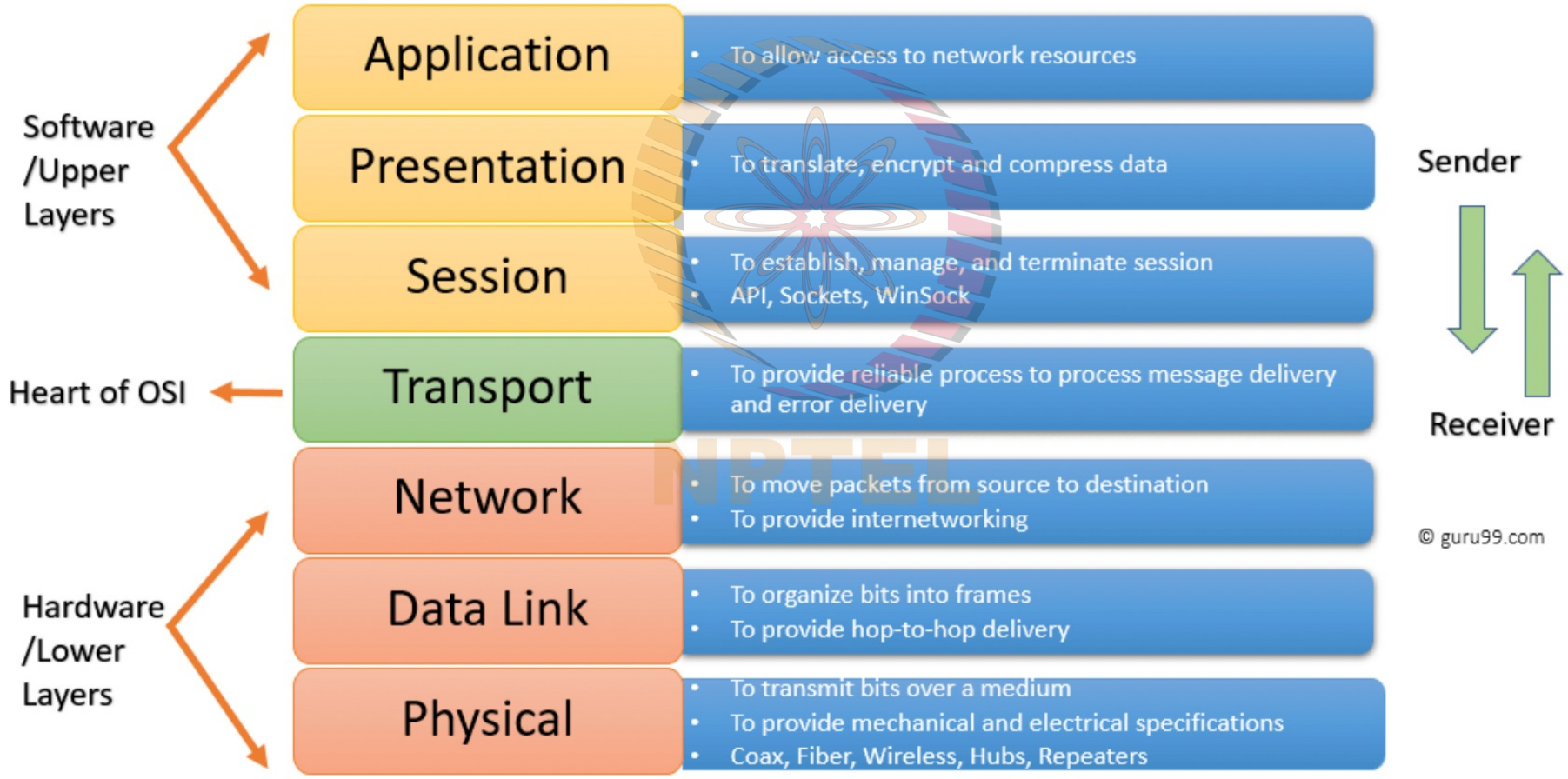


Actual Design of a SHA 256.

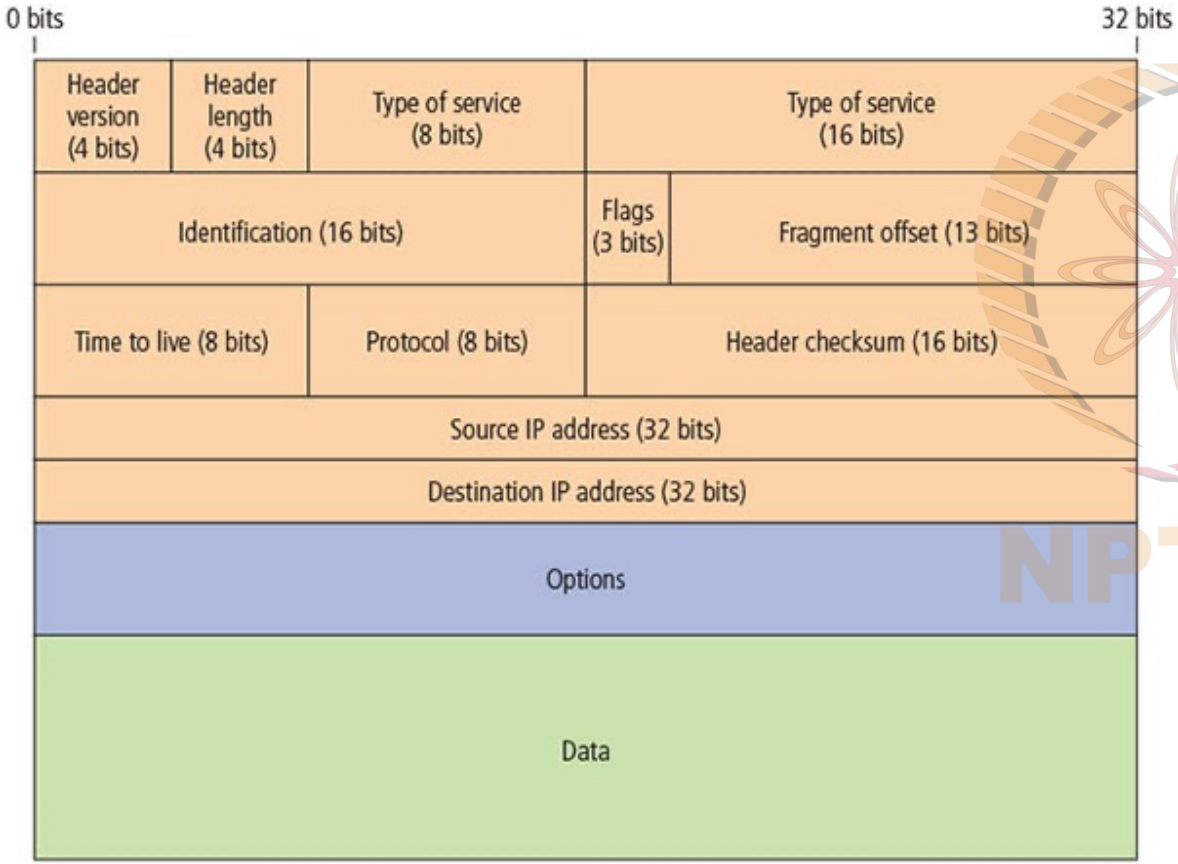
Introduction to Concepts : Cyber Security

- General Concepts
  - Operating Systems
  - Cryptography
- **Networking Concepts**
  - OSI Model
  - Packets & Protocols
  - Firewalls
  - Design of a Simple Network
- Security Concepts
  - CIA Triad
  - Connecting to Network
  - Cyber Operational Concepts & Terms.
- Workshop & Discussion
  - QBOT : Execution
  - QBOT : Analysis

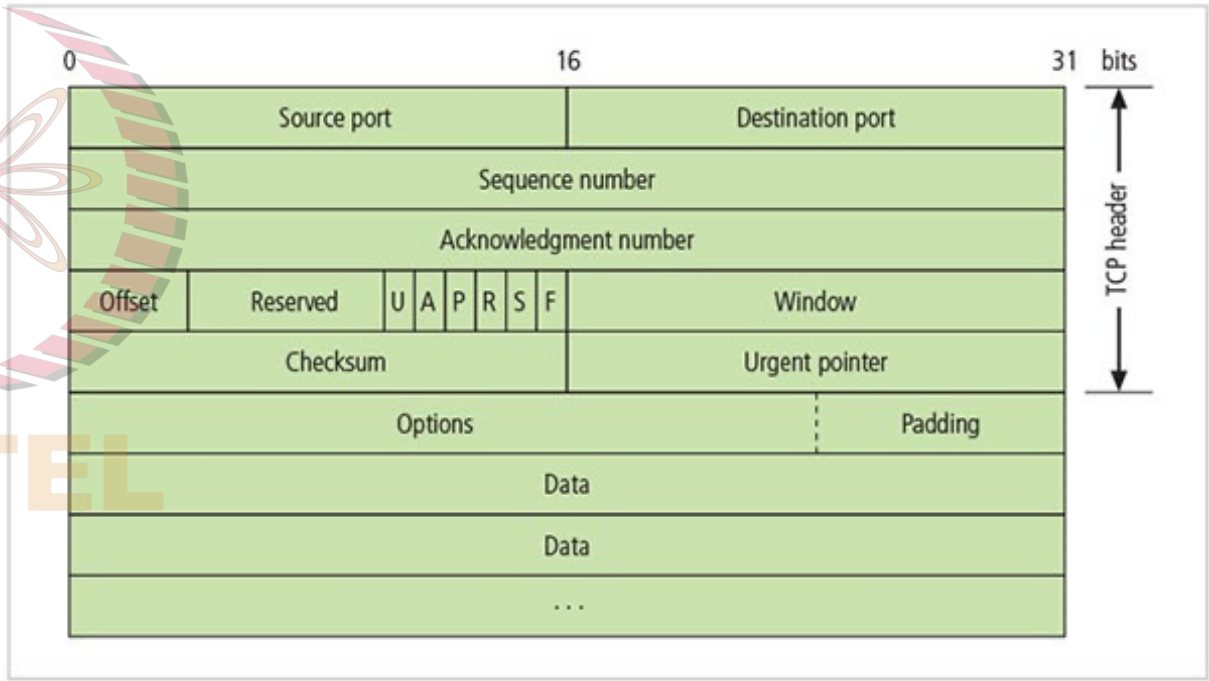
OSI Model : Network Layers.



Network Packets.

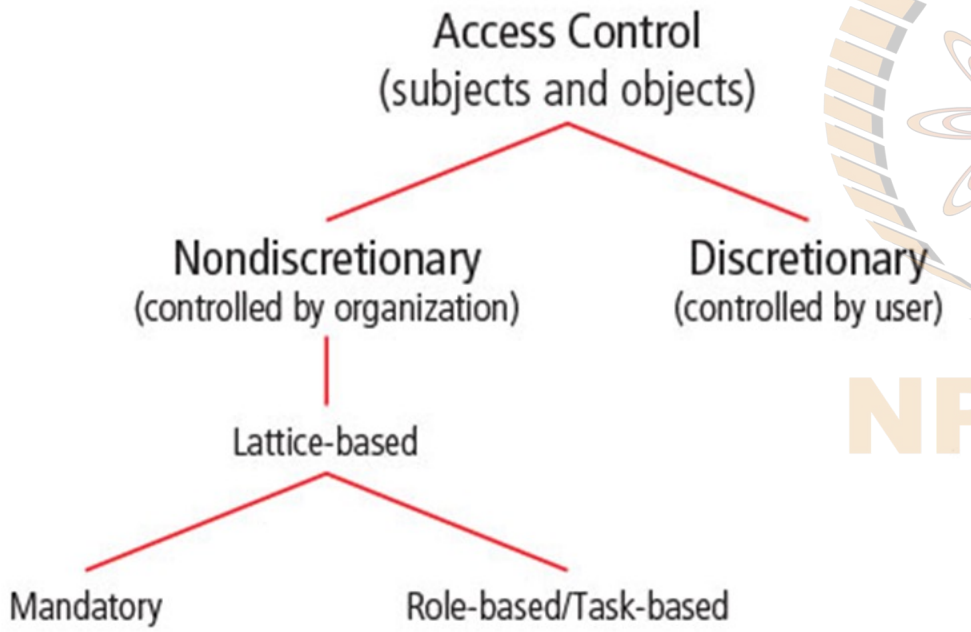


IP Packet



TCP Packet

Access Controls.



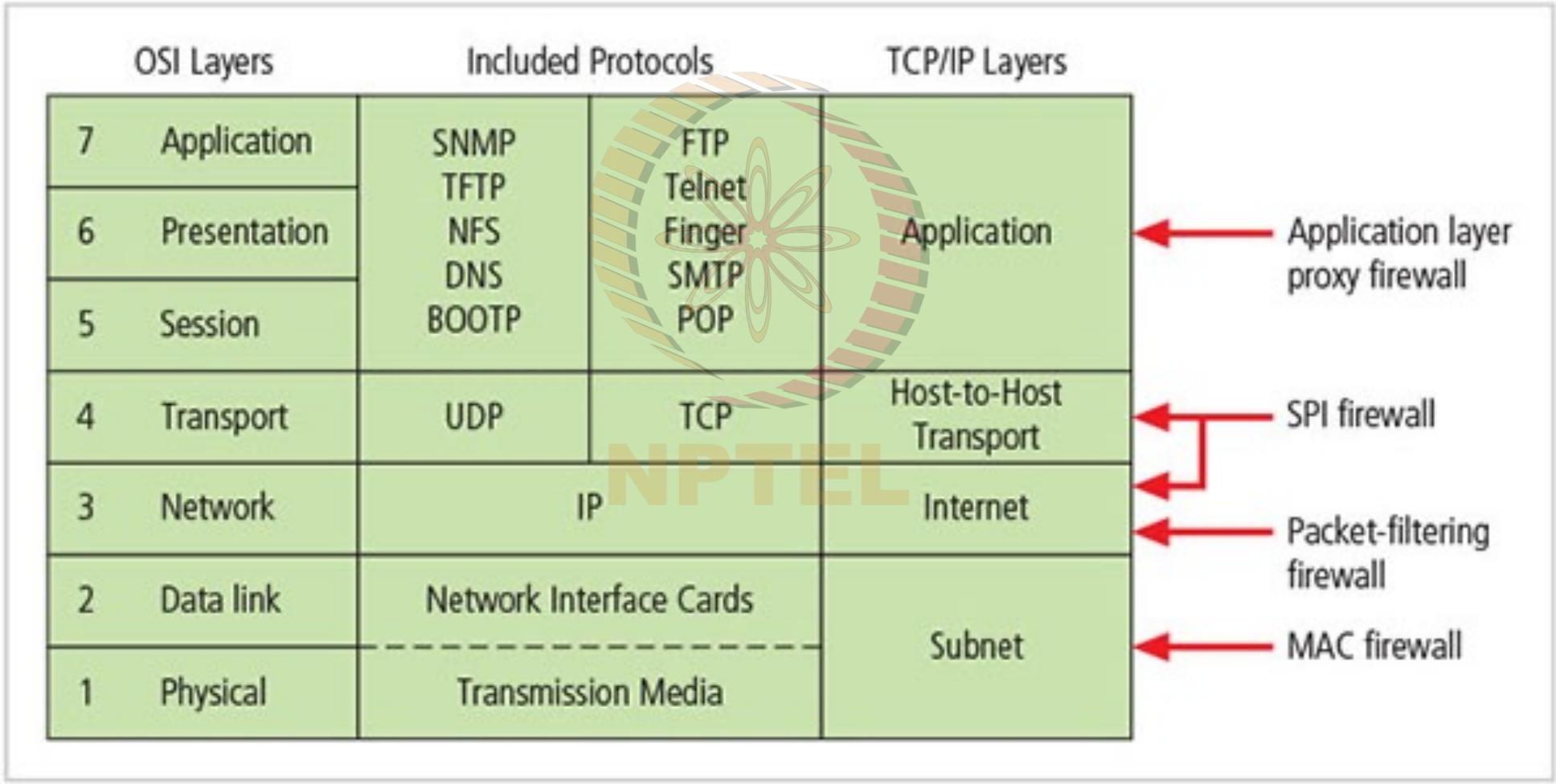
Security Checks.

Largely implemented through Lists.

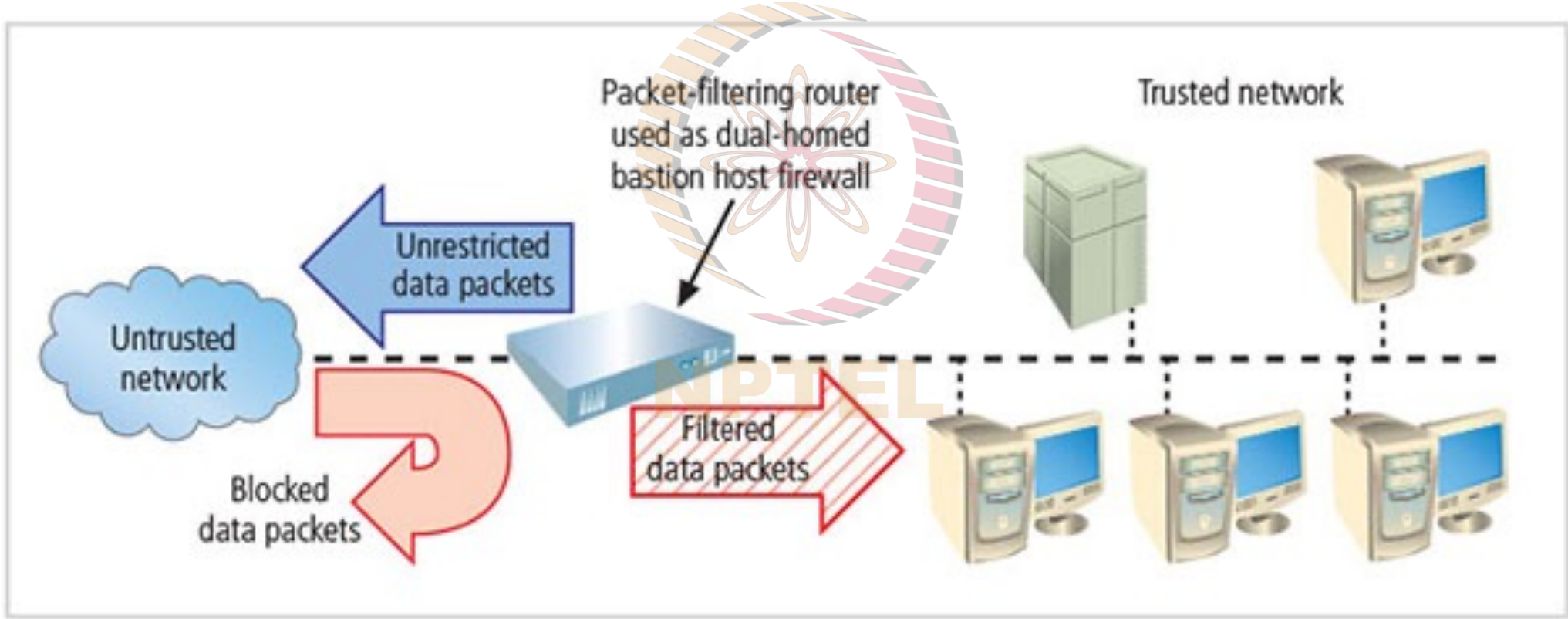
Identity and Access Management Solutions cover this issue.

- LDAP
- Kerberos
- Radius Server

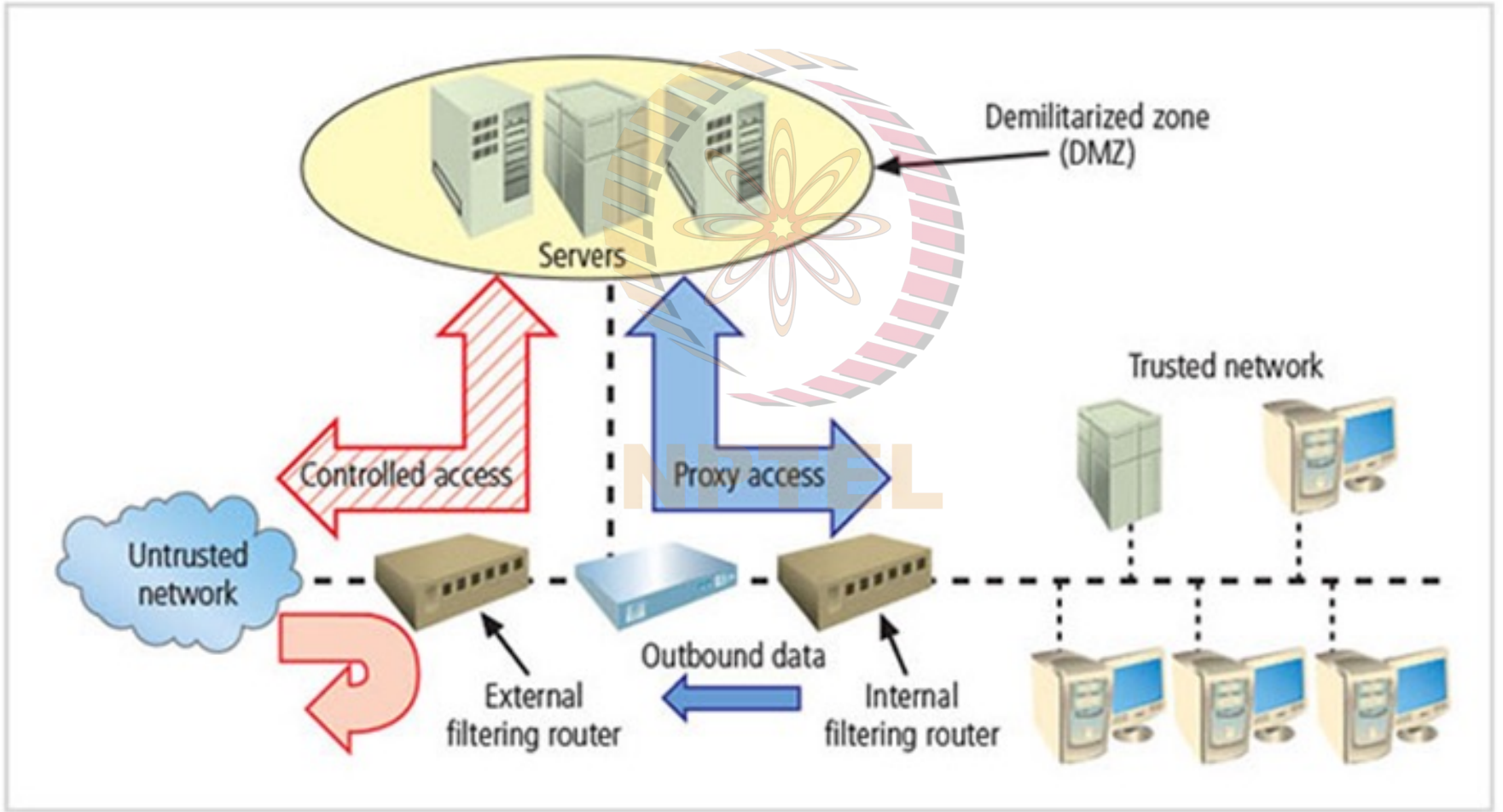
Firewalls.


OSI Layers
Included Protocols
TCP/IP Layers
7 Application
6 Presentation
5 Session
SNMP
TFTP
NFS
DNS
BOOTP
FTP
Telnet
Finger
SMTP
POP
Application
4 Transport
UDP
TCP
Host-to-Host Transport
3 Network
IP
Internet
2 Data link
Network Interface Cards
1 Physical
Transmission Media
Subnet
Application layer proxy firewall
SPI firewall
Packet-filtering firewall
MAC firewall

Packet Filtering Router : Basic Firewall.

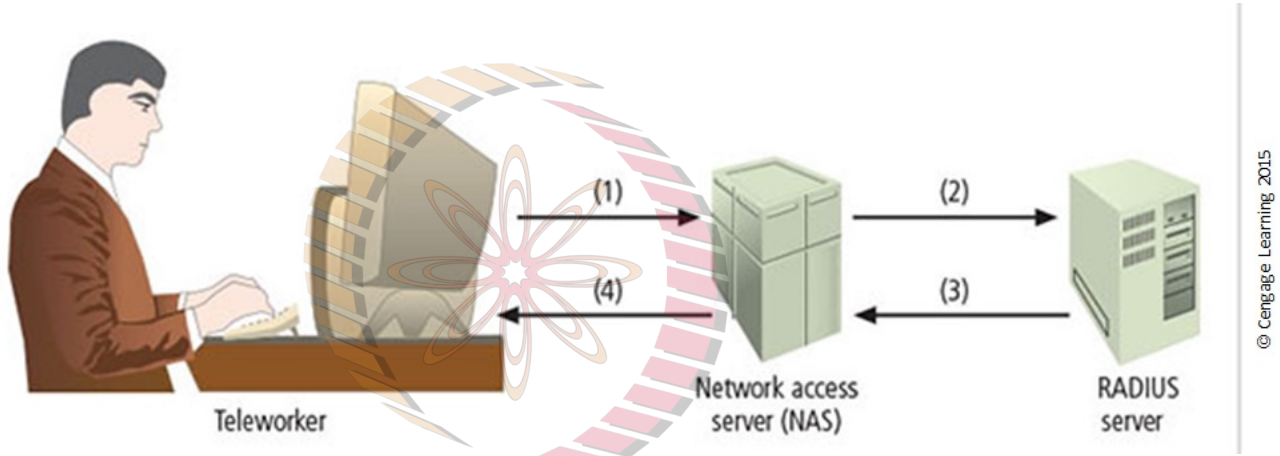


Regular Corporate Networks

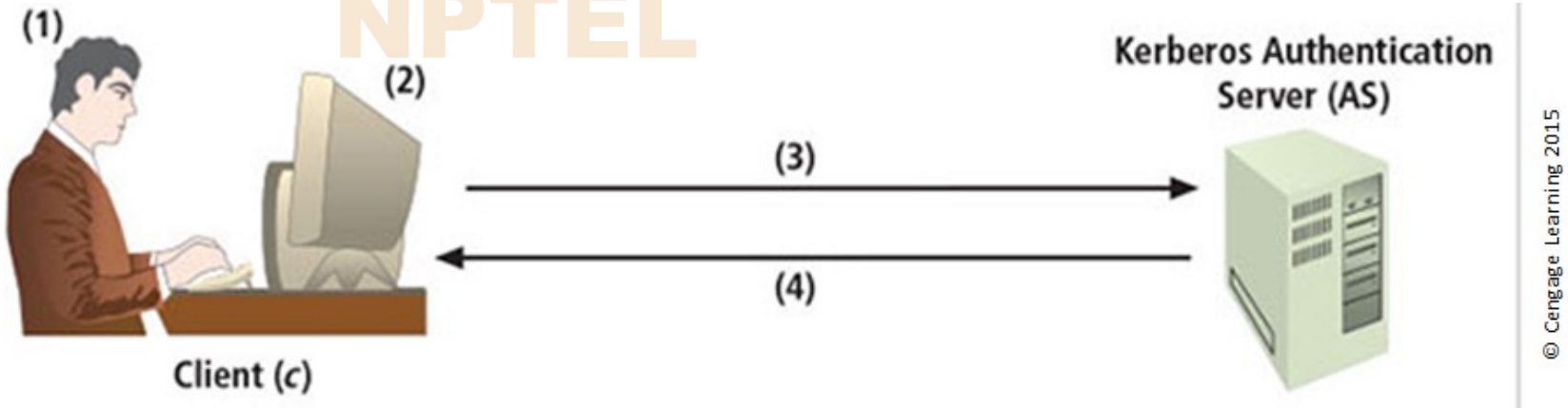


Connecting from Outside.

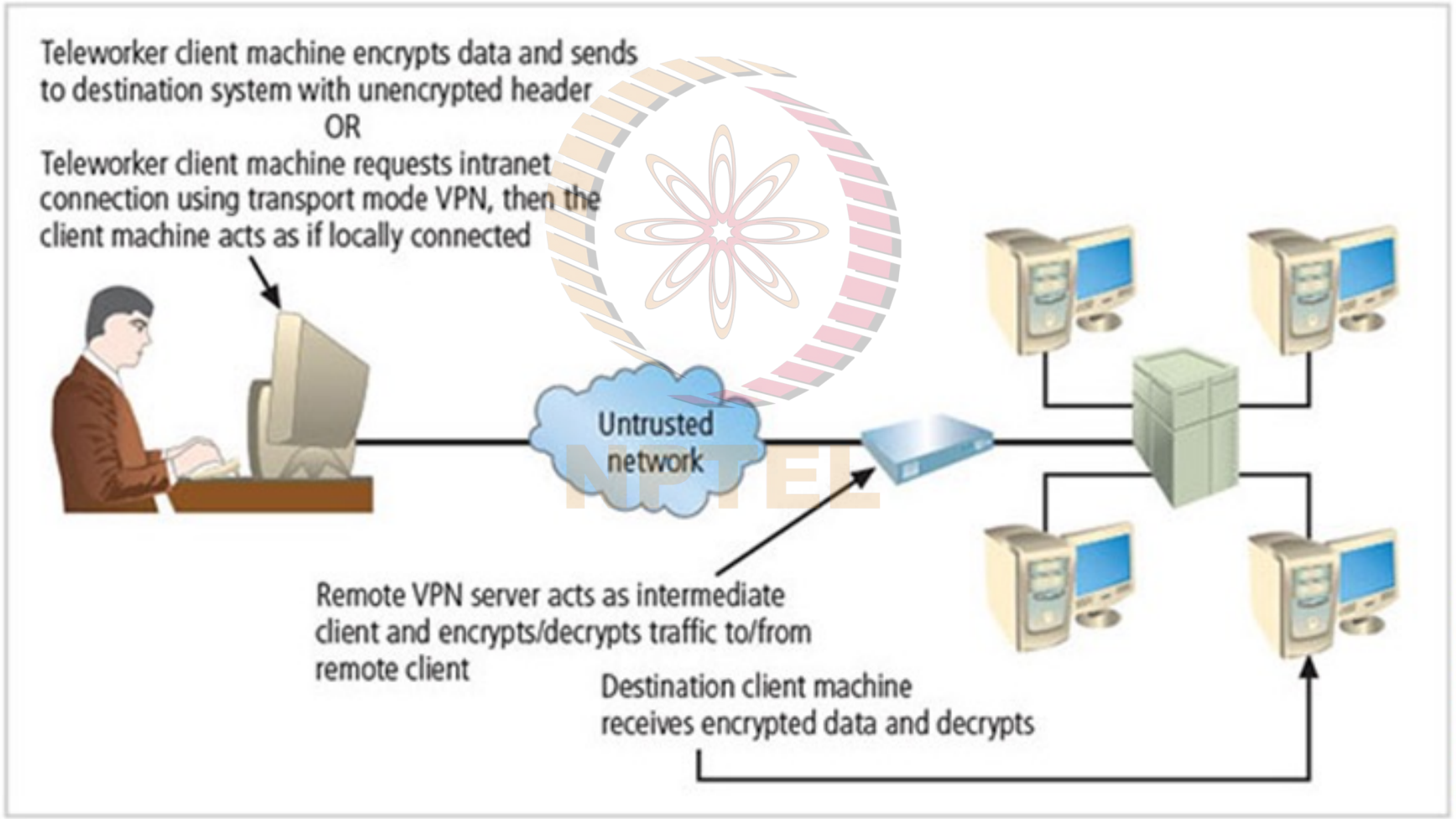
1



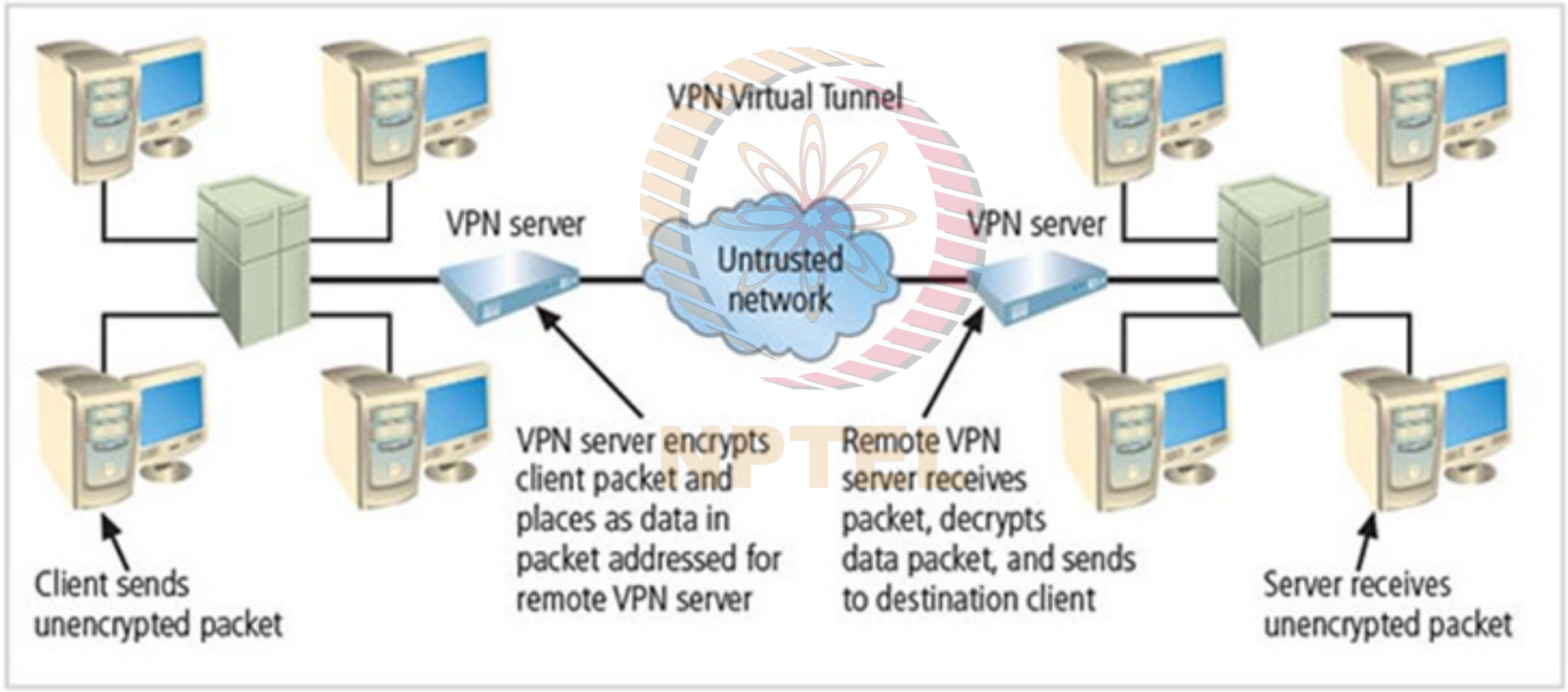
2



VPN – Virtual Private Network



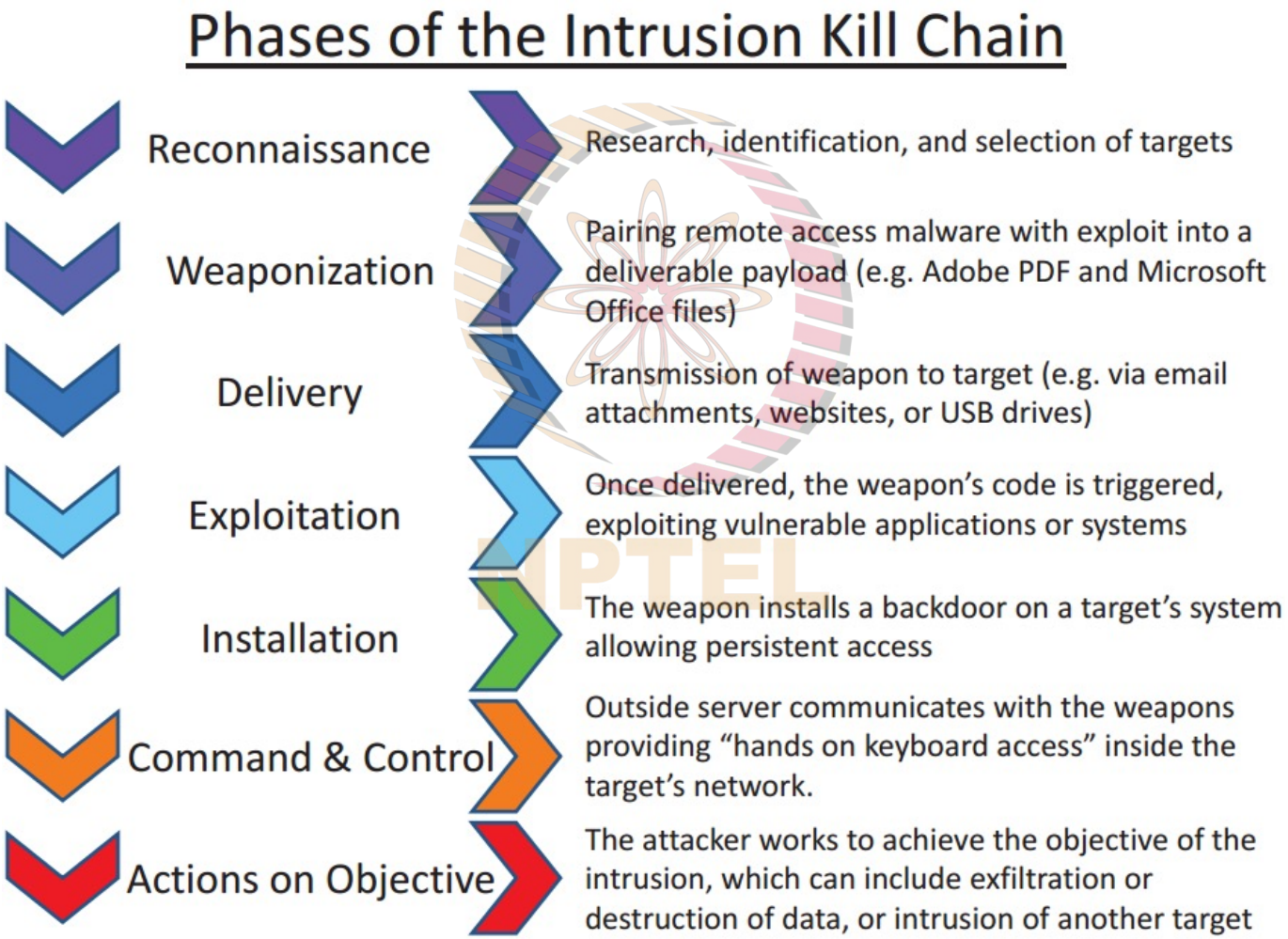
VPN : Connecting Two Networks



Introduction to Concepts : Cyber Security

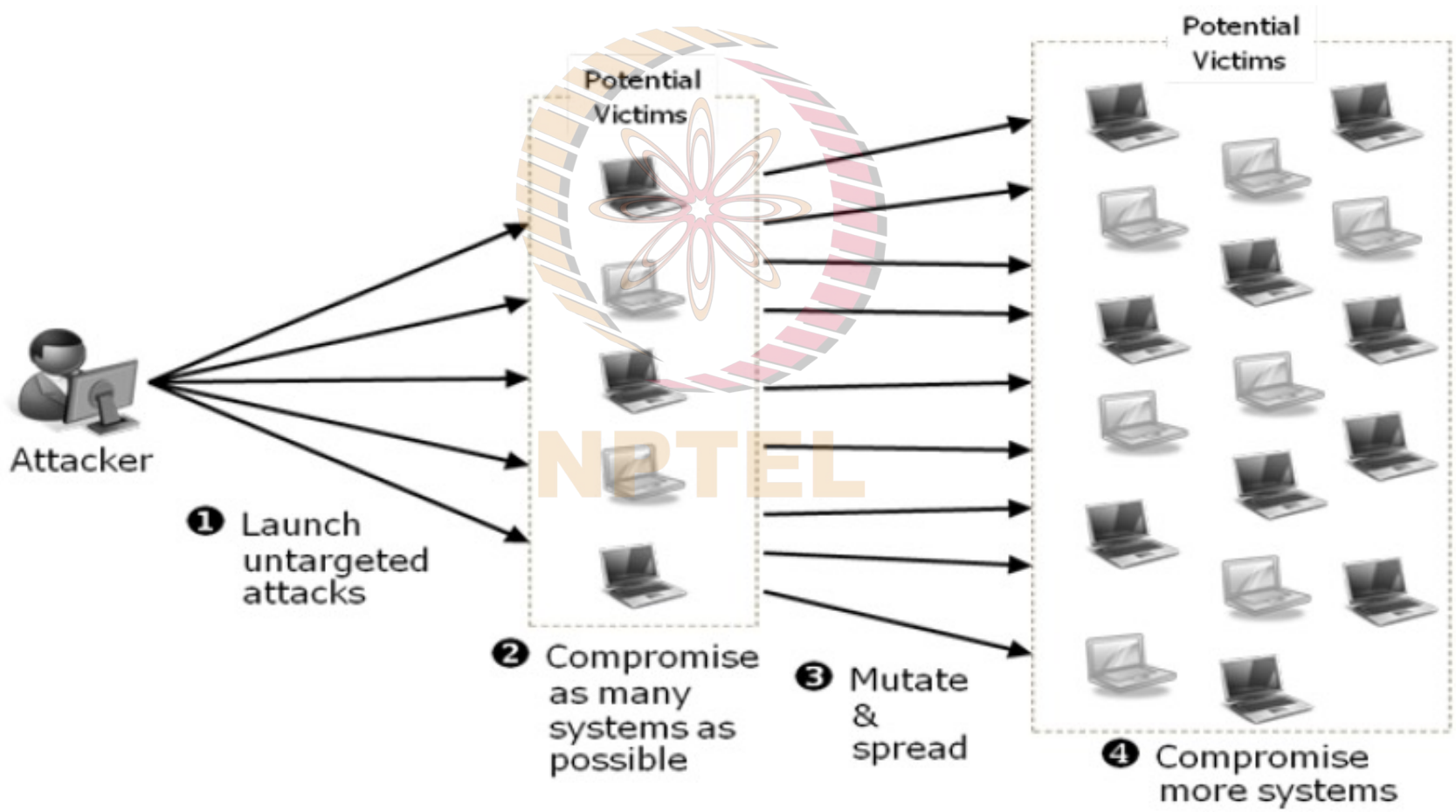
- General Concepts
  - Operating Systems
  - Cryptography
- Networking Concepts
  - OSI Model
  - Packets & Protocols
  - Firewalls
  - Design of a Simple Network
  - Connecting to Network
- **Security Concepts**
  - CIA Triad
  - Cyber Operational Concepts & Terms.
- Workshop & Discussion
  - QBOT : Execution
  - QBOT : Analysis

Cyber Attack : Phases.

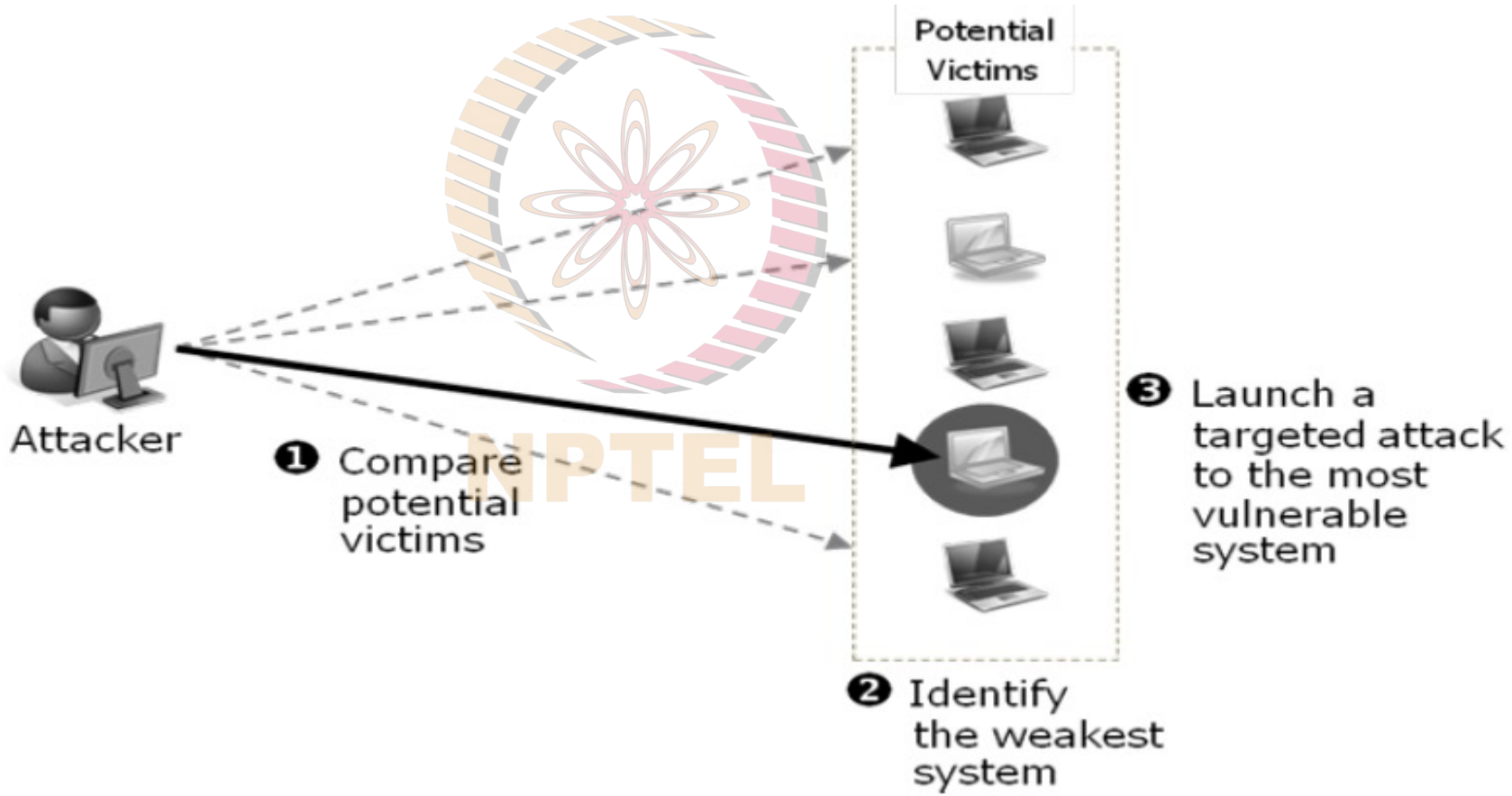


General Information Collection strategies.

Untargeted Attacks



Focussed Information Collection.



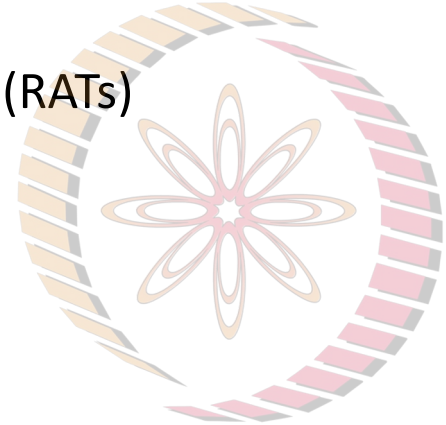
Targeted Attacks

Basic Concepts

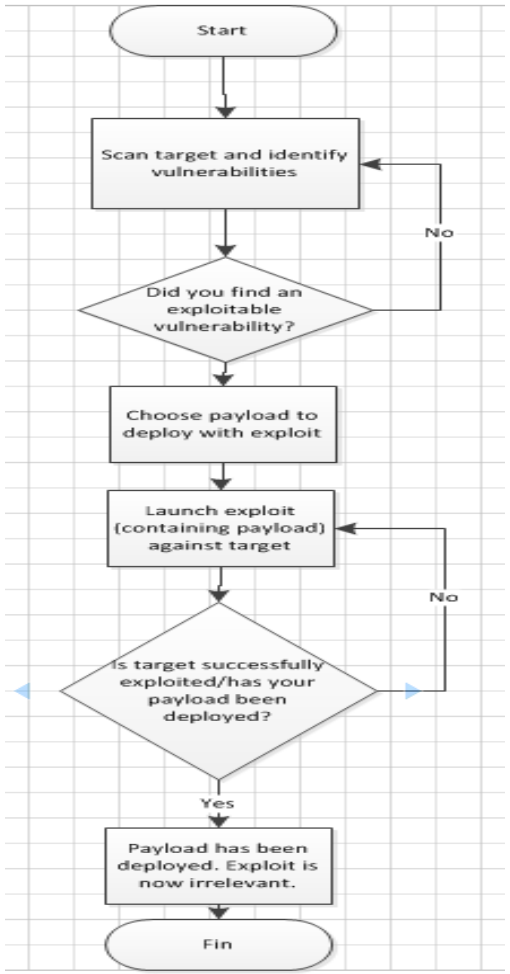
- **Confidentiality**
  - Keeping data hidden for unauthorized users.
  - Example : Encryption.
- **Integrity**
  - Accuracy and completeness of the data.
  - Example : Hash matches & Checksums
- **Availability**
  - Being able to access the data when required.
  - Example: Denial of Service Attacks

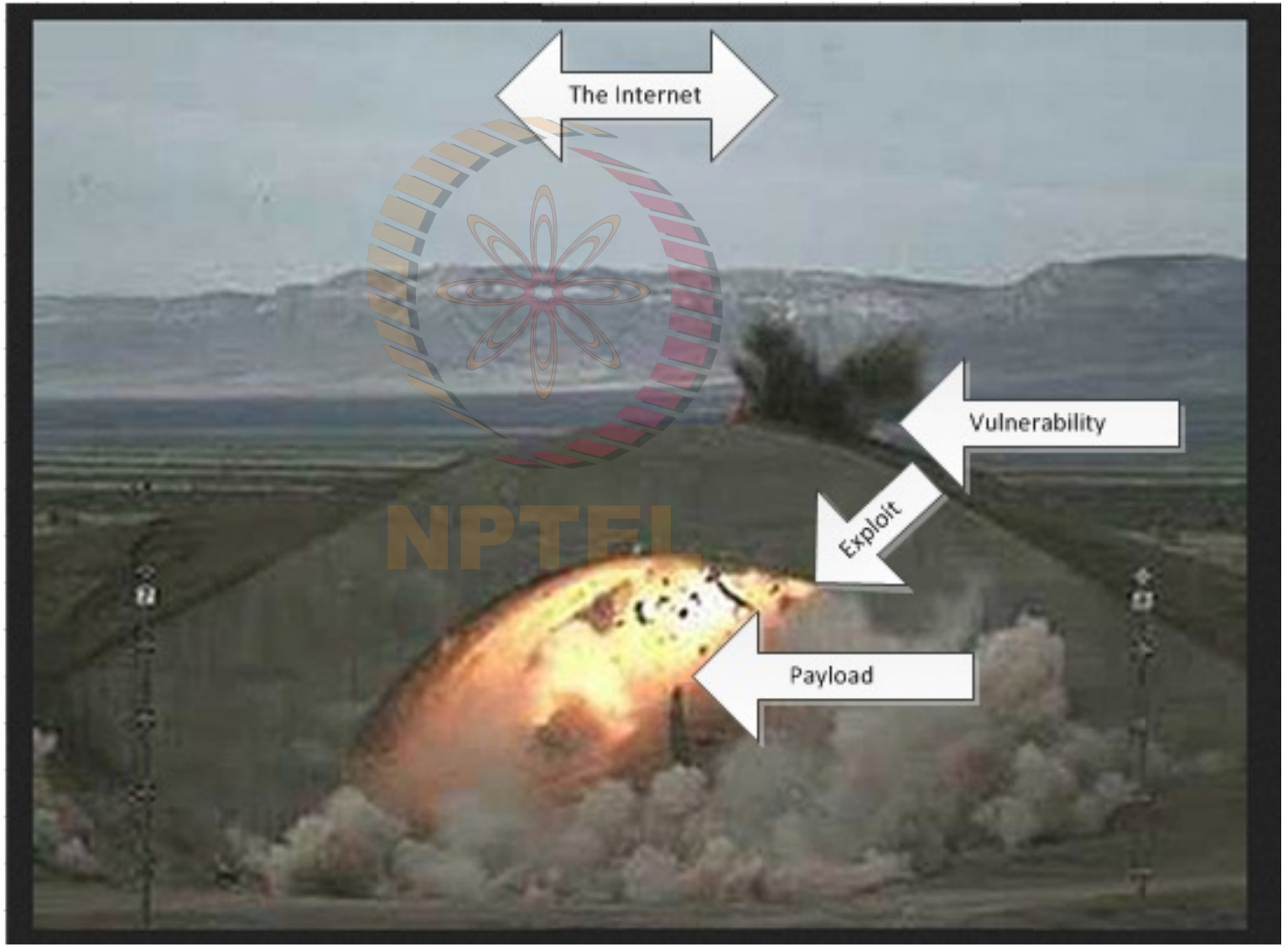
Common Terminologies.

- Malware.
  - Remote Administration Tools (RATs)
  - Trojans.
  - KeyLogger.
  - Ransomware.
- Social Engineering
  - Phishing & Spear Phishing.
- Command & Control (C2)
- “Man in the Middle” (MitM) attack.
- Denial of Service attack
- Distributed Denial of Service Attack (DDoS).



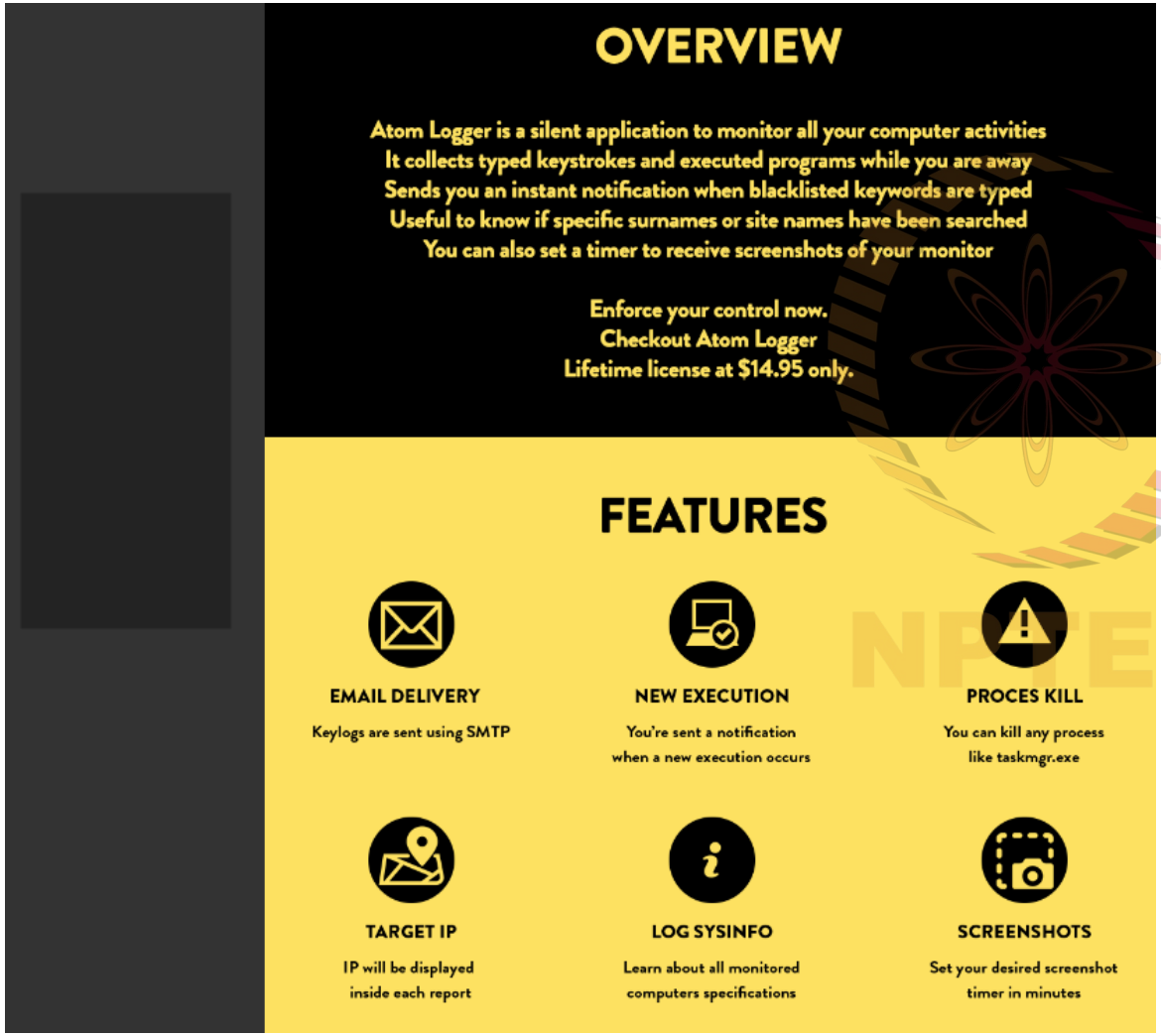
Concepts of Ethical Hacking.





- Scanning
- Vulnerability
- Exploit
- Payload

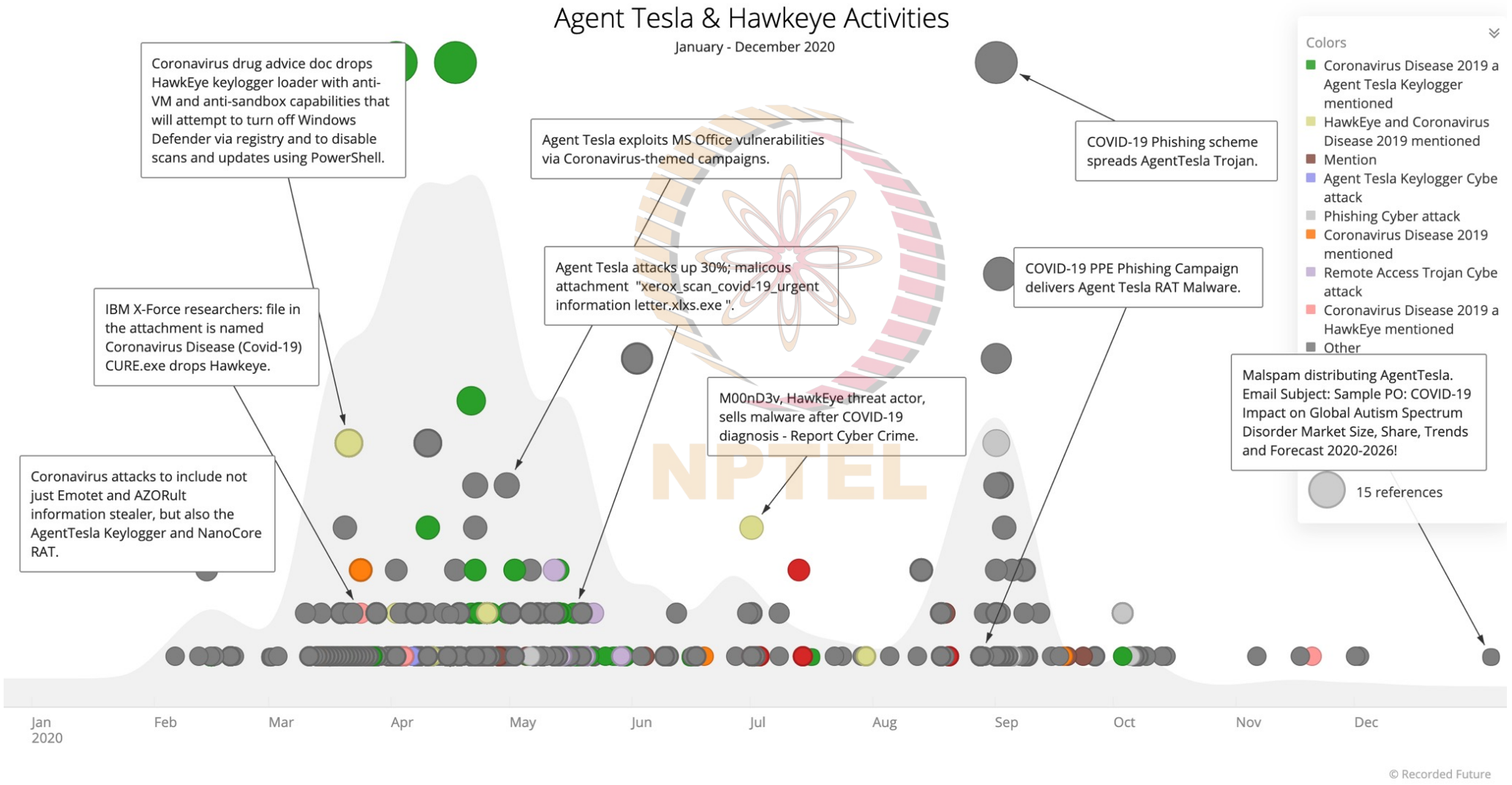
Remote Administration Tool.



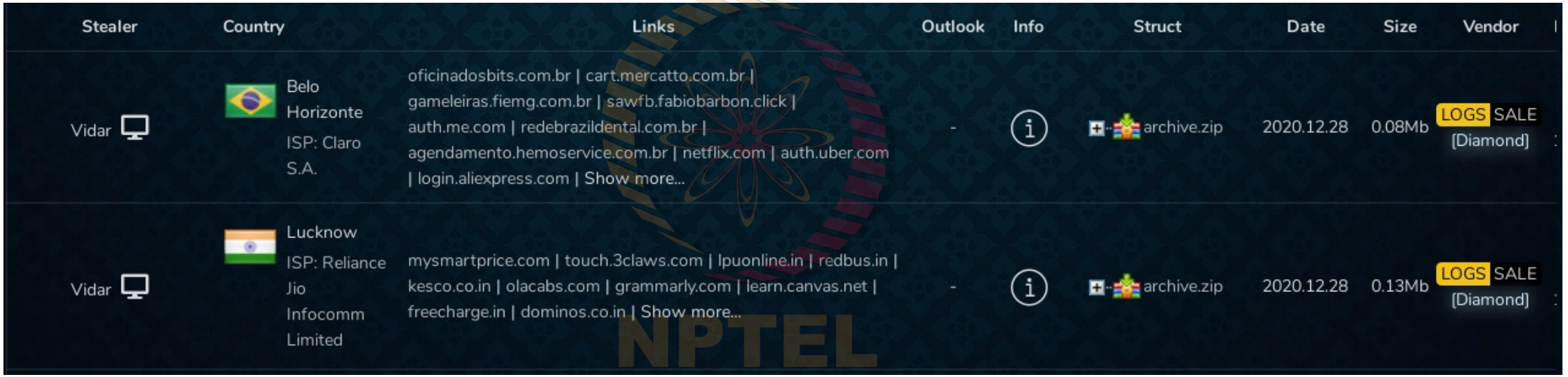
$14.95 USD only.

- Multiple Options.
- Commercial Tools (Misused)
  - Ammy Admin
  - Team Viewer
  - AnyDesk
- Professional & Open Source
  - Puppy RAT
  - Qrat
- Professional & Licensed
  - DarkComet
  - Atom Logger (See Screen.)

Post-Covid use of Key Loggers.



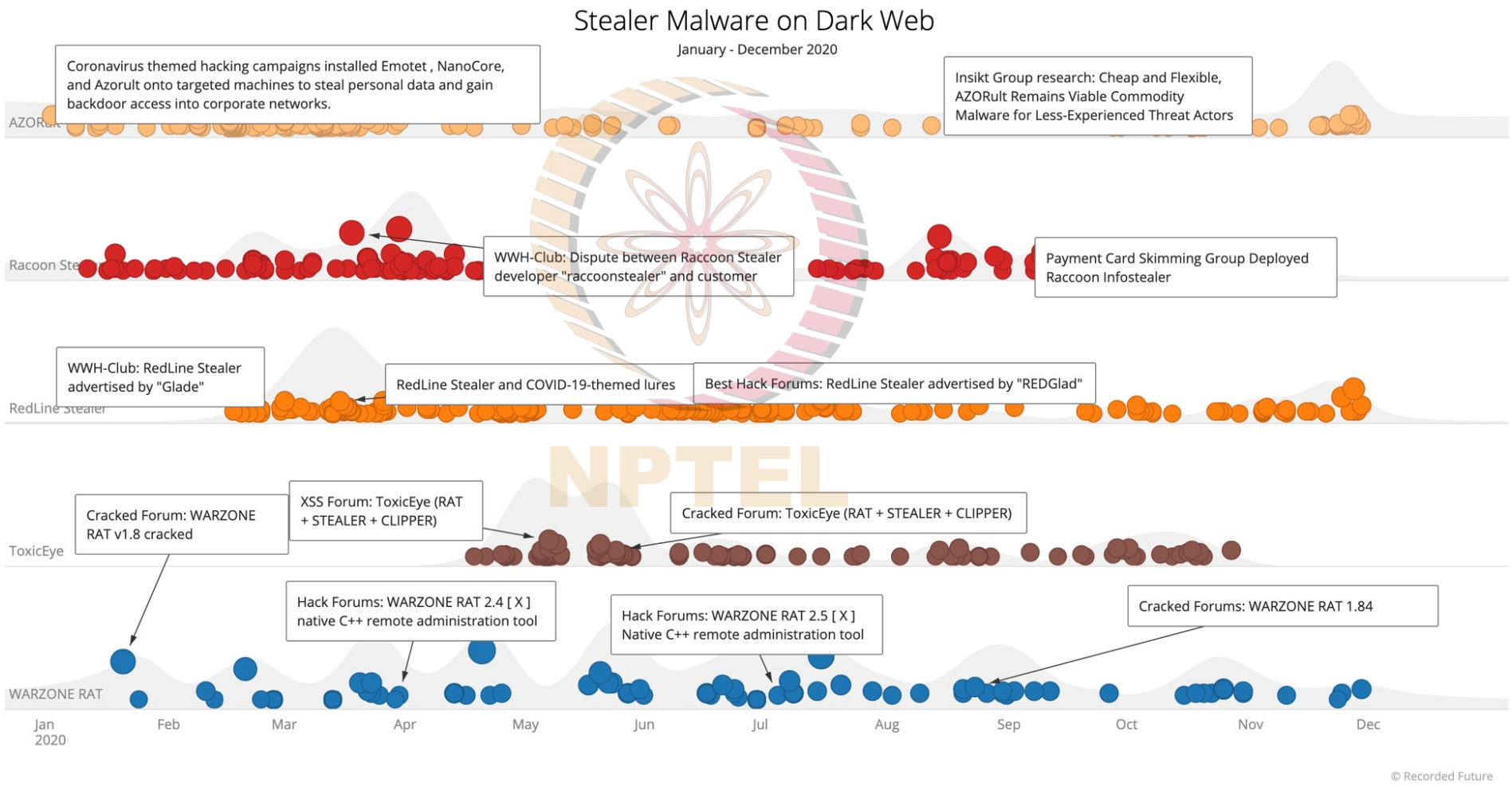
Command & Control Panels.



Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor
Vidar	Belo Horizonte ISP: Claro S.A.	oficinadosbits.com.br | cart.mercatto.com.br | gameleiras.fiemg.com.br | sawfb.fabiobarbon.click | auth.me.com | redebrazildental.com.br | agendamento.hemoservice.com.br | netflix.com | auth.uber.com | login.aliexpress.com | Show more...	-		archive.zip	2020.12.28	0.08Mb	LOGS SALE [Diamond]
Vidar	Lucknow ISP: Reliance Jio Infocomm Limited	mysmartprice.com | touch.3claws.com | lpuonline.in | redbus.in | kesco.co.in | olacabs.com | grammarly.com | learn.canvas.net | freecharge.in | dominos.co.in | Show more...	-		archive.zip	2020.12.28	0.13Mb	LOGS SALE [Diamond]

Panel for seeing Victims : Command & Control.

Supply Sources.



India also has a vibrant dark web market.

Increased Attack Surface.

Amazon Alexa security bug allowed access to voice history

13 August 2020

Critical Zoom vulnerability triggers remote code execution without user input

The researchers who discovered the bug have earned themselves $200,000.

By Charlie Osborne for Zero Day | April 9, 2021 -- 10:15 GMT (15:45 IST) | Topic: Security

A zero-day vulnerability in Zoom which can be used to launch remote code execution (RCE) attacks has been disclosed by researchers.

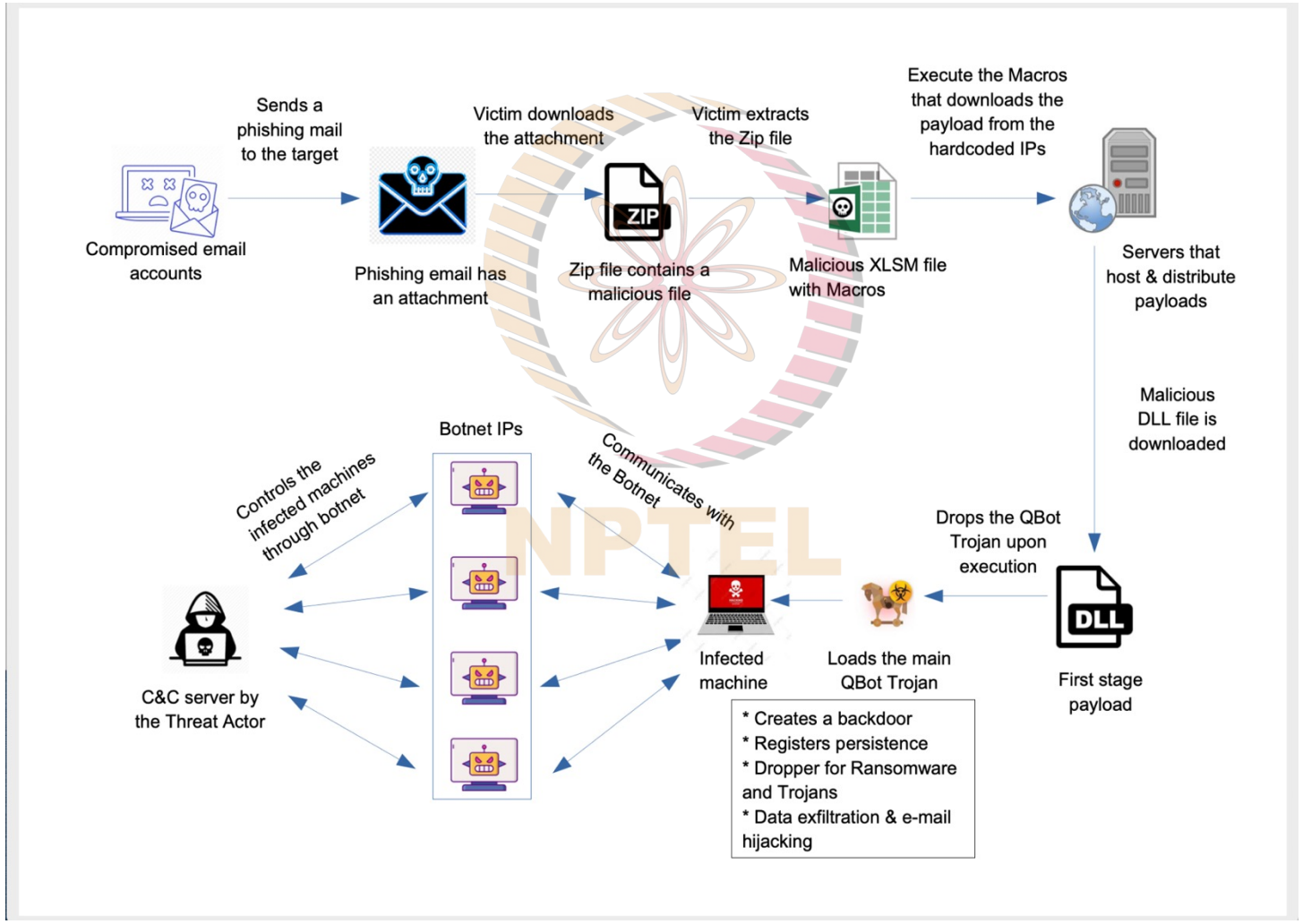
Google is indexing WhatsApp group chat links, making even private groups discoverable

A Twitter user discovered the flaw that would let anyone join any WhatsApp group chat

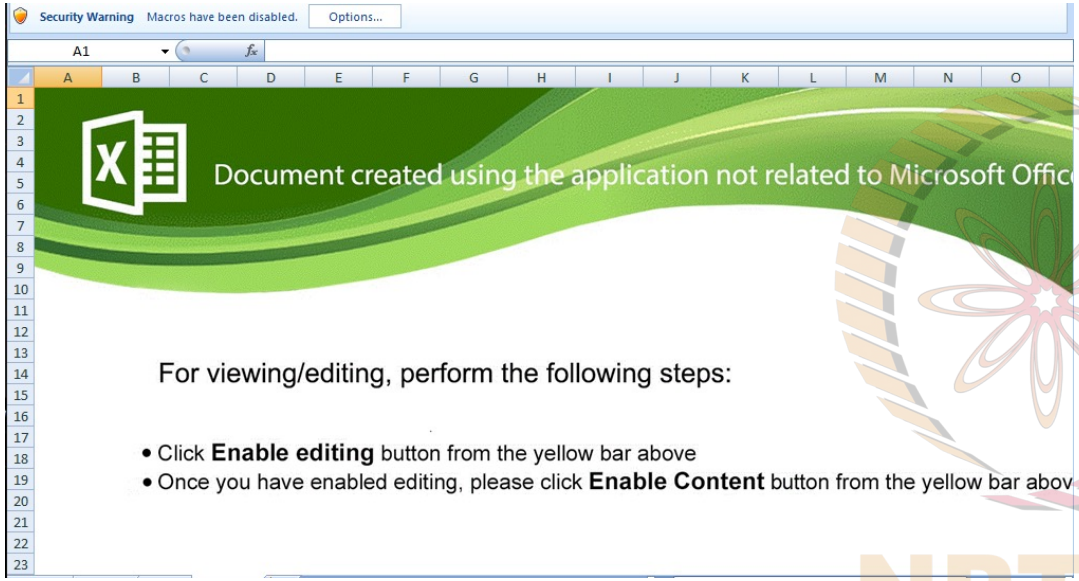
By Kim Lyons | Feb 21, 2020, 1:06pm EST

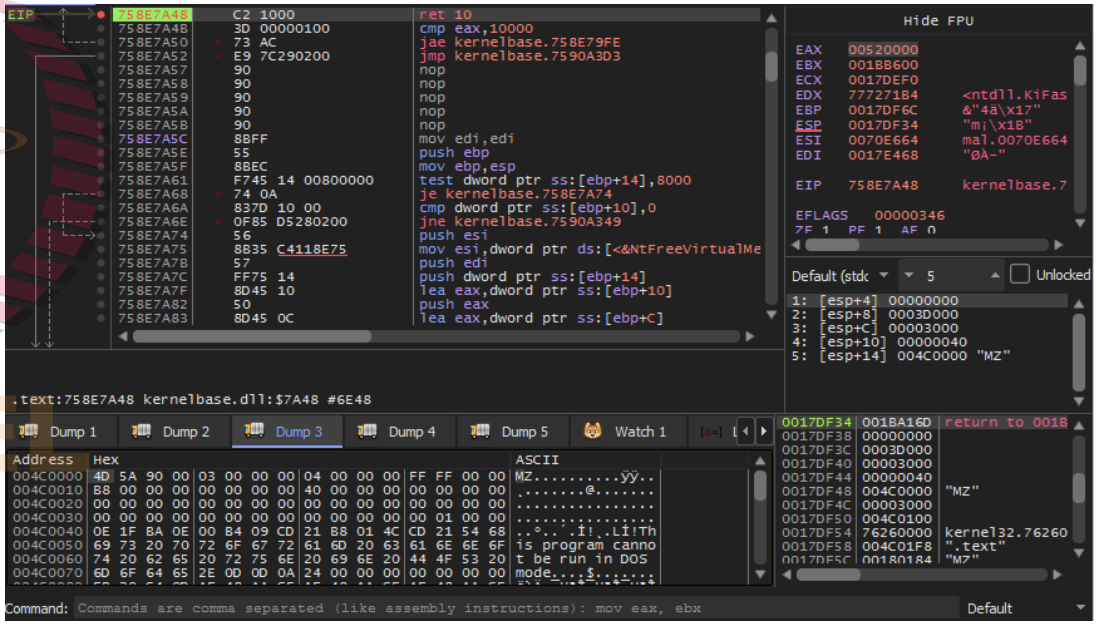
Evaluation of the QBOT Trojan.

QBOT Trojan


Compromised email accounts
Sends a phishing mail to the target
Phishing email has an attachment
Victim downloads the attachment
Zip file contains a malicious file
Victim extracts the Zip file
Malicious XLSM file with Macros
Execute the Macros that downloads the payload from the hardcoded IPs
Servers that host & distribute payloads
Malicious DLL file is downloaded
First stage payload
Drops the QBot Trojan upon execution
Loads the main QBot Trojan
Infected machine
Botnet IPs
Controls the infected machines through botnet
Communicates with the Botnet
C&C server by the Threat Actor
* Creates a backdoor
* Registers persistence
* Dropper for Ransomware and Trojans
* Data exfiltration & e-mail hijacking

Analysis of the Malware.






```
<sheet name="Sheet" sheetId="2" r:id="rId1"/>
<sheet name="Sheet1" sheetId="13" r:id="rId2"/>
<sheet name="Sheet2" sheetId="14" r:id="rId3"/>
<sheet name="Pervi" sheetId="3" state="hidden" r:id="rId4"/>
<sheet name="Pervi2" sheetId="4" state="hidden" r:id="rId5"/>
<sheet name="sobr" sheetId="5" state="hidden" r:id="rId6"/>
<sheet name="sobr1" sheetId="6" state="hidden" r:id="rId7"/>
<sheet name="sobr2" sheetId="7" state="hidden" r:id="rId8"/>
<sheet name="sobr3" sheetId="8" state="hidden" r:id="rId9"/>
<sheet name="zap1" sheetId="9" state="hidden" r:id="rId10"/>
<sheet name="zap2" sheetId="10" state="hidden" r:id="rId11"/>
<sheet name="zap3" sheetId="11" state="hidden" r:id="rId12"/>
<sheet name="osn" sheetId="12" state="hidden" r:id="rId13"/>
```

What is a Cyber Attack?

- A cyber-attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage.

Hackers	APT Groups
Aim for Financial Gains, Notorious activities. Example: Compromising Bank Account, Defacement.	Aims to gain access to critical infrastructure for information **A - Advanced** **P - Persistence** **T - Threat** Example: Corona Virus Vaccination Development

Motive of an APT Group

- Steal Data
  - Adversaries Development
  - Intelligence
  - To Plan Future Action
- Disrupt the operations
  - Economic Loss
- Destroy the infrastructure
  - Business Continuation

China's cyberattack on Maharashtra power grid was to improve PLA's bargaining position

China's cyber assault against India's critical infrastructure in October 2020 happened amid an ongoing crisis on their contested boundary.

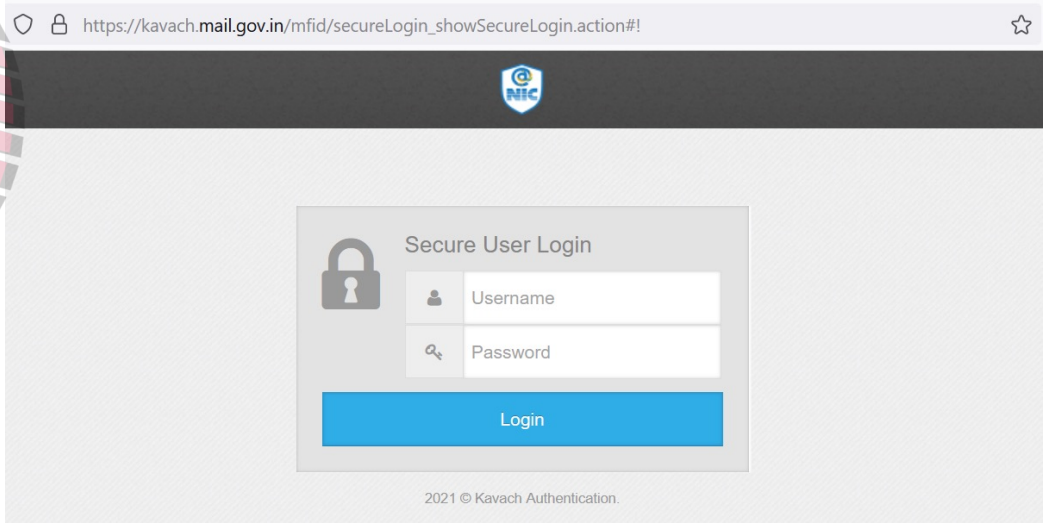
Top Cyber-Attack trends

Malware (short for **“malicious software”**) is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. ... Investigate the infected user's local network. Steal sensitive data.

Top Threats 2019-2020		Assessed Trends
1	Malware	----
2	Web-based Attacks	----
3	Phishing	↗
4	Web application attacks	----
5	Spam	↙
6	Denial of service	↙
7	Identity theft	↗
8	Data breaches	----
9	Insider threat	↗
10	Botnets	↙
11	Physical manipulation, damage, theft and loss	----
12	Information leakage	↗
13	Ransomware	↗
14	Cyberespionage	↙
15	Crytojacking	↙

SideCopy : An APT Group.

- Operation SideCopy is active from early 2019, till date with Chinese help.
- This cyber-operation has been only targeting Indian defense forces and armed forces personnel.
- Malware modules seen are constantly under development and updated modules are released after a reconnaissance of victim data.
- Actors are keeping track of malware detections and updating modules when detected by AV.
- This threat actor is misleading the security community by copying TTPs that point at Sidewinder APT group.



Some of the Organised Crime Groups.

- Cobalt Cybercrime Gang
- Lazarus Group
- MageCart Syndicate
- Evil Corp
- GozNym Gang
- DarkSide
- REvil
- Clop
- Lapsus$
- FIN7

Lapsus$

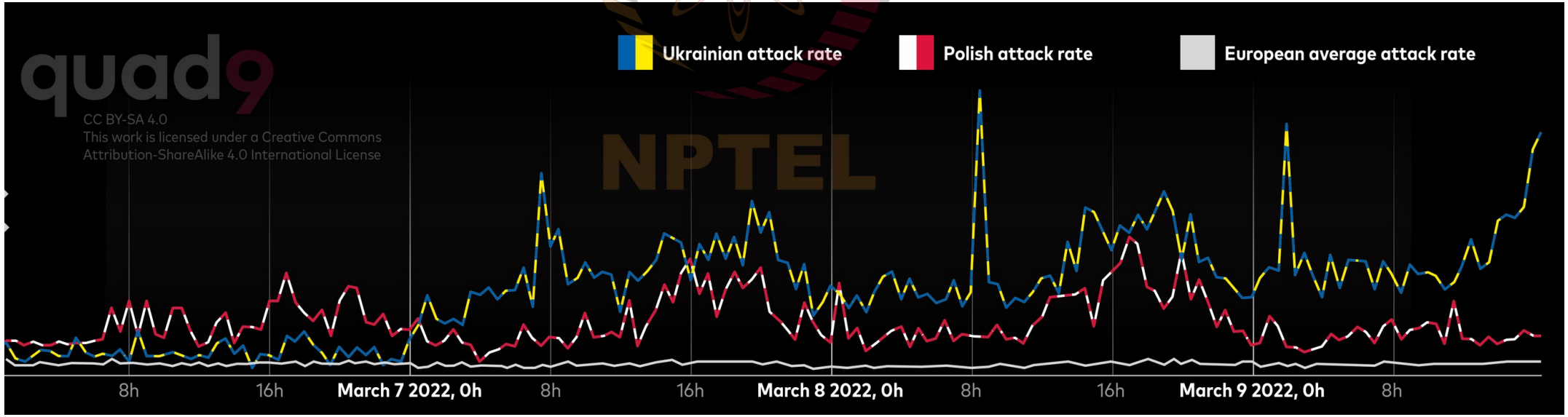
- Lapsus$, stylised as LAPSUS$ and classified by Microsoft as DEV-0537, is an international extortion-focused hacker group known for its various cyberattacks against companies and government agencies
- In March 2022, Lapsus$ gained notoriety for a series of cyberattacks against large tech companies, including Microsoft, Nvidia and Samsung
- Following these attacks, the City of London Police announced that it had made seven arrests in connection to a police investigation into Lapsus$.
- Although the group had been considered inactive by April 2022, the group is believed to have re-emerged in September 2022 with a series of data breaches against various large companies through a similar attack vector, including Uber and Rockstar.

Russia Ukraine Cyberwarfare

- During the prelude to the 2022 Russian invasion and even during the invasion multiple cyberattacks against Ukraine were recorded, as well as some attacks on Russia.
- The first major cyberattack took place on 14 January 2022, and took down more than a dozen of Ukraine government websites
- According to Ukrainian officials, around 70 government websites, including the Ministry of Foreign Affairs, the Cabinet of Ministers, and the Security and Defense Council, were attacked. Most of the sites were restored within hours of the attack
- On 15 February 2022, a large DDoS attack brought down the websites of the defense ministry, army, and Ukraine's two largest banks, PrivatBank and Oschadbank .Cybersecurity monitor Netblocks reported that the attack intensified over the course of the day, also affecting mobile apps and ATMS of the banks
- Independent hacker groups, such as Anonymous, have launched cyberattacks on Russia in retaliation for the invasion

Russia Ukraine Cyberwarfare

- Beginning on 6 March, Russia began to significantly increase the frequency of its cyber-attacks against Ukrainian civilians.
- On 9 March alone, the Quad9 malware-blocking recursive resolver intercepted and mitigated 4.6 million attacks against computers and phones in Ukraine and Poland, at a rate more than ten times higher than the European average.



Introduction to Securing Institutions.

Cyber Attack of accident?

October 12 blackout was a sabotage

By Abhishek Sharan / Updated: Nov 20, 2020, 08:04 IST

FACEBOOK TWITTER LINKEDIN EMAIL

Photo by Deepak Turbhekar

A source in the government said hackers have been trying to target the country's power utilities since February.

Last month's power outage in the Mumbai Metropolitan Region (MMR) was possibly the result of a sophisticated sabotage attempt involving foreign entities, a probe carried out by the state police's cyber cell has revealed.

The month-long probe detected presence of multiple "suspicious log – ins" into the servers connected with power supply and transmission utilities by accounts operating from Singapore and a few other south Asian countries. The state police is now coordinating with national agencies to determine if these "intrusions, interferences" were part of a coordinated effort aimed at crippling the country's financial capital.

Control system failure caused phosphine leak

TNN | Jan 30, 2011, 00:35 IST

A- A+

TOI

LUCKNOW: Failure of the chemical reaction control system in the chemical factory is believed to behind the phosphine gas leak, which led to death of three persons in the Sandila industrial area on Saturday. Over two dozen people have also fallen sick due to the incident, which occurred in the early morning hours.

The five member team constituted by the district magistrate (DM), Hardoi, AKS Rathore, will now find out that whether the chemical reaction system failure was due to lack of safety measures in the plant, poor upkeep of the equipments or sabotage.

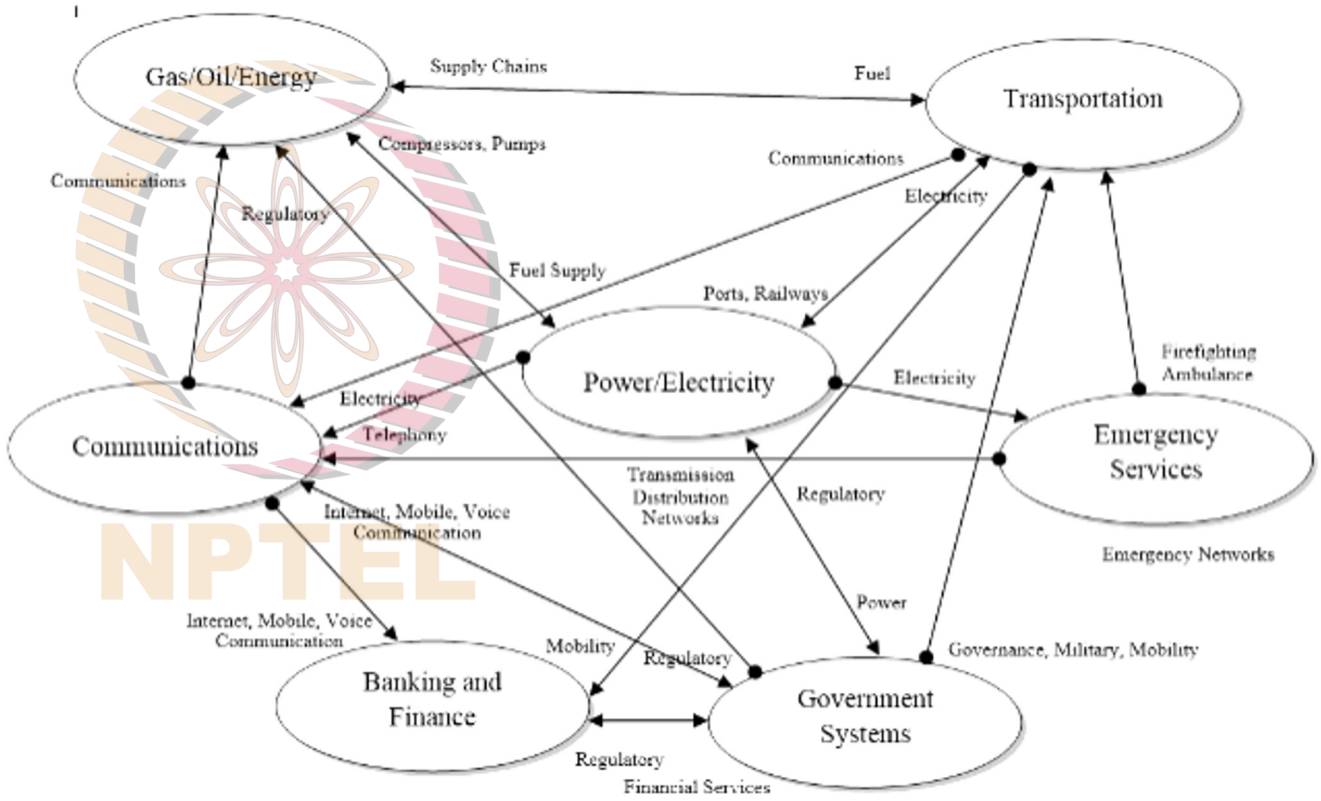
What is Critical information infrastructure?

- “Critical Information Infrastructure (CII) is defined as those facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation”

Information Technology Act as amended in 2014.

What are Critical sectors?

- Power & Energy
- Banking, Financial Services & Insurance
- Telecom
- Transport
- Government
- Strategic & Public Enterprises



QUICK STUDY OF RECENT ATTACKS

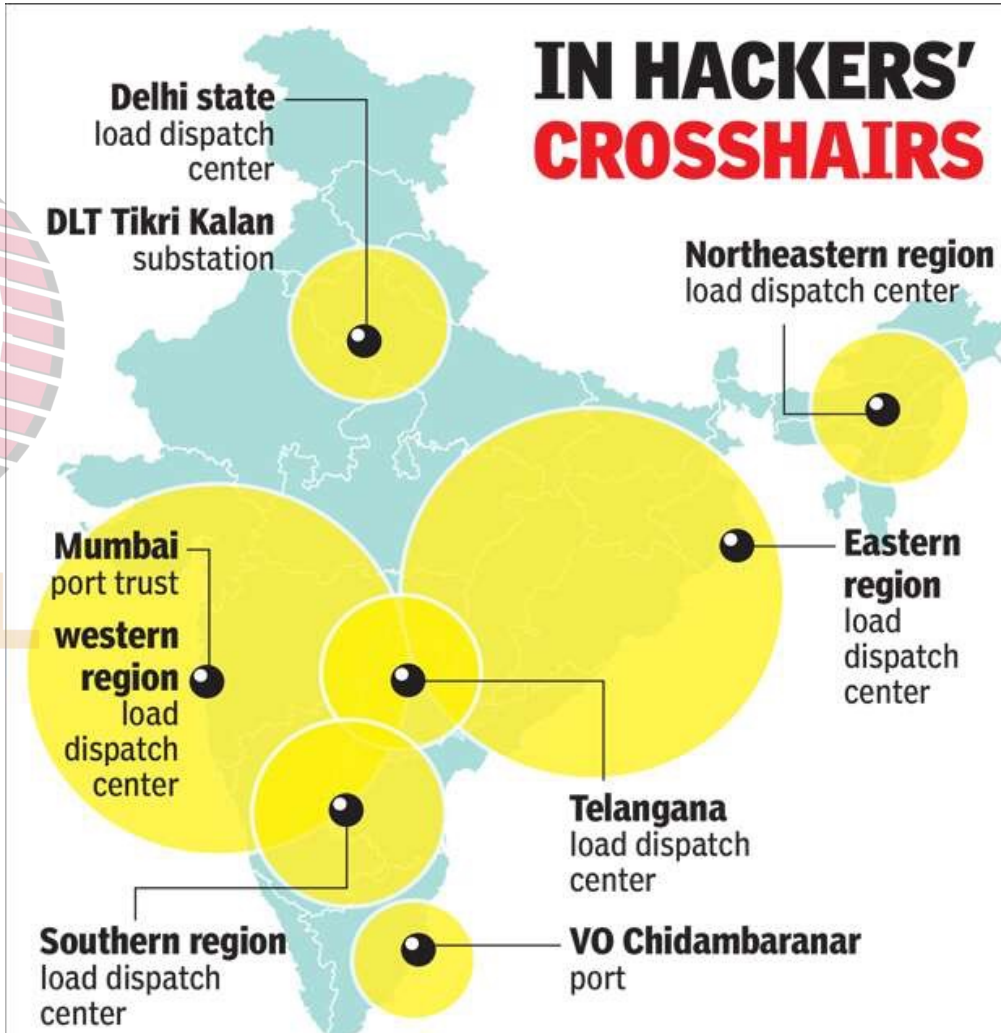
Sno	Cyber Attack	Possible Espionage Objectives	Possible Warfare Objectives
1	Air India	Monitor Movements & Visits of Diplomats and Senior Functionaries	Logistics, Public Morale, Economic Loss.
2	Nucleus Software	Monitor Financial & Economic health of the country	Supply Chain Attack on the Banking infrastructure possible.
3	Dominos and UpStox	Personal Details of Whos Who leaked.	Track and compromise - surgical cyber strikes on specific personnel.
4	SII and Bharat Bio-tech	Steal IPR to improve their vaccine.	Disrupt and destory - reputation as pharma power, morale of people, economy and recovery from pandemic.
5	Mobikwik	Monitor Financial & Economic health of the country	Track and compromise - surgical cyber strikes on specific personnel.
6	Airtel - J&K (Airtel Denied.)	Personal Details of Who-is-Who in JK for cyber ops -- imagine impact with widespread Chinese Mobile Phones - Resolve identities.	Track and compromise - surgical cyber strikes on specific personnel.
7	JusPay	Monitor Financial & Economic health of the country	Track and compromise - surgical cyber strikes on specific personnel.
8	Bigbasket	Personal Details of Whos Who leaked.	Track and compromise - surgical cyber strikes on specific personnel.

QUICK STUDY OF RECENT ATTACKS

Sno	Cyber Attack	Possible Espionage Objectives	Possible Warfare Objectives
9	Dr Reddy Laboratories	Steal IPR to improve their vaccine.	Disrupt and destory - reputation as pharma power, morale of people, economy and recovery from pandemic.
10	Tata Power - Mumbai	Demonstrate Capability to see our response.	Disrupt and destory - confidence in Govt, morale of people, economy and recovery from pandemic.
11	Indian Railways	Monitor Military and Frieght Movement (Northern Railways)	Joint Operation with Pakistan - Possible human element involved.
12	Unacademy	Understanding preferences of youth.	Create psychological impact on youth - as a country which is weak and vulnerable.
13	Kudankulam Nuclear Power Plant	Steal IPR and monitor the possible production of fissile material - an idea on Nuclear Capabilities.	Triggering an accident - could be devastating in our country.
14	ISRO	Monitor our moon program and steal sensitive data on payloads.	Create psychological impact on youth, world - as a country which is incompetent, weak and vulnerable.
15	Healthcare Data Leaked	Helps companies in customising sales strategies for Indian Market.	Not much.

Mumbai Power Grid Attack

- Industrial Sector – Power Grid
- Threat Source - Adversarial/ Nation - State
- Attack Motivation - Sabotage / Reputational
- Attack Scope - Cyber-Physical
- Attack Domain - Software/Hardware/ Communications/ Supply Chain
- Attack Mechanism - Manipulate System Resource
  Inject Unexcepted Items
- Attack Type - Active
- Targeted Principle - Integrity



What is (NCIIPC) ?

- National Critical Information Infrastructure Protection Centre (NCIIPC) is an organisation of the Government of India created under Sec 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16 January 2014.
- It is based in **New Delhi**, **India.**
- It is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection.
- It is a unit of the National Technical Research Organisation (NTRO).

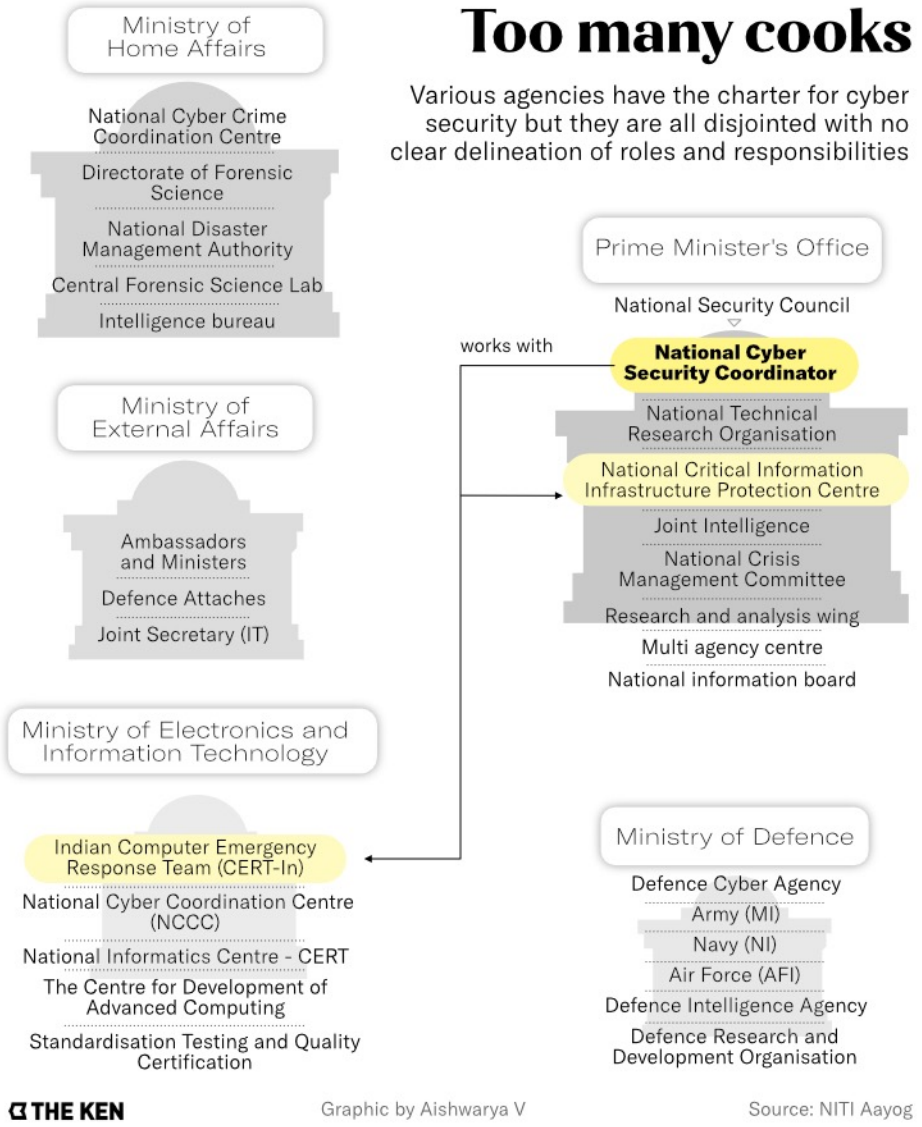
"To take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders. "

* Notifies - Protected System.
* Issues - Audit Guidelines

Critical infrastructures

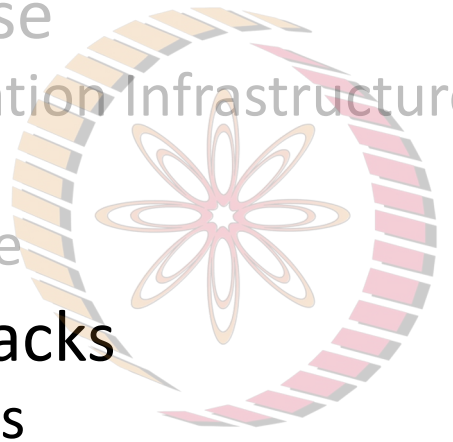
Lack of CLARITY.

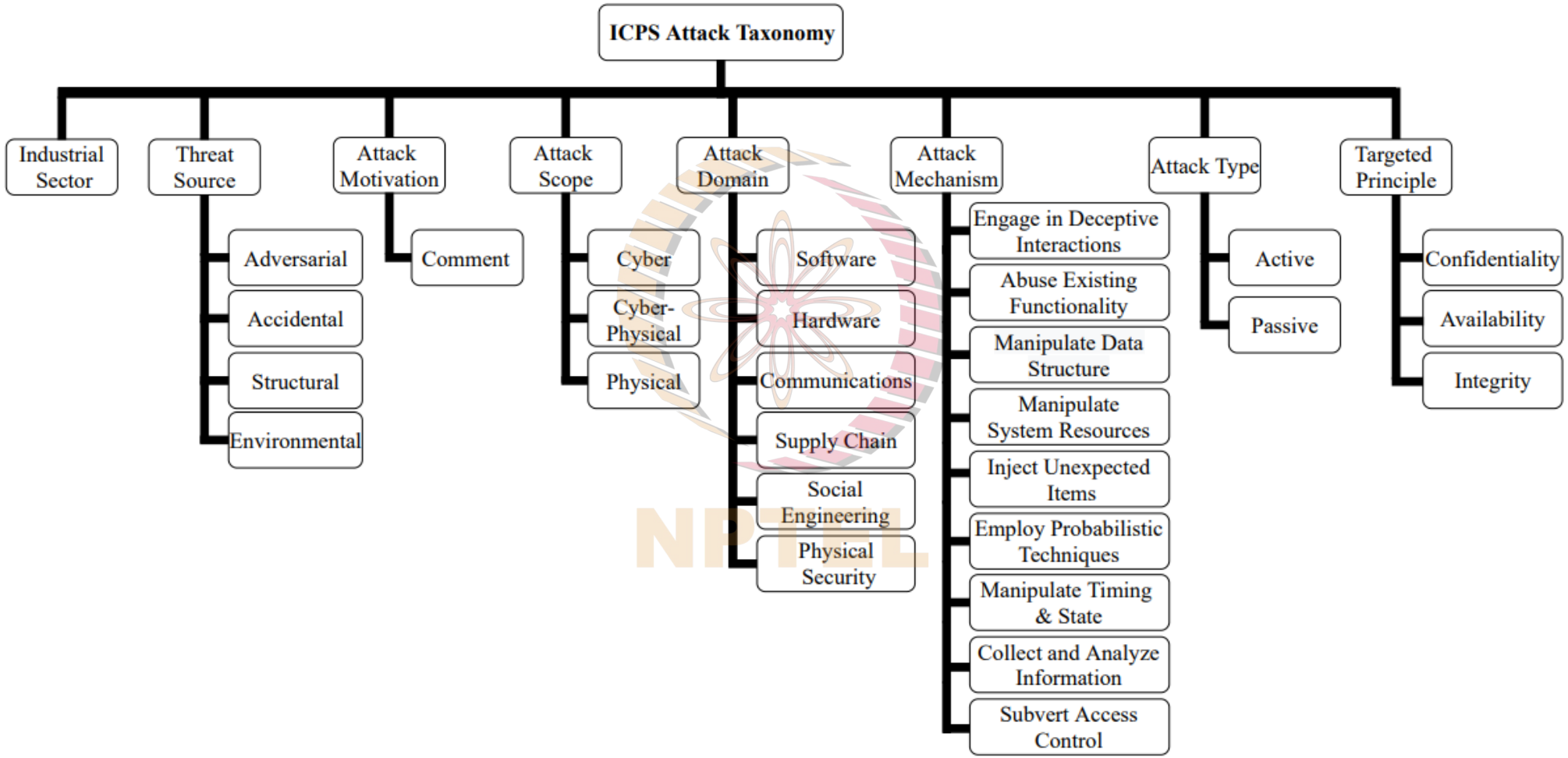
- Multiple Players attempting to regulate.
- Stakeholders are totally confused on whose directions to implement.
- Precious resources are divided between the various government departments.
  - Botnet cleaning center appears to be a preventive job.
  - NCCC monitors the networks of CIIs.
  - NIC & Telecom Departments have their critical role in CIIP.
- Standardisation teams exist for each agency separately.
  - STQC exists and largely covers Hardware testing for performance and not security testing.



Introduction to Securing Institutions.

- Concepts for Cyber Defense
  - Concept of Critical Information Infrastructure
  - Attacks on India
  - Indian Regulatory Structure
- Study of Cyber Kinetic Attacks
  - Framework to study attacks
  - Attacks on CIIPs from World.
- Defending Institutions
  - Securing the Agency
  - Securing the Infrastructure
  - Use of Threatintel from Cyberspace.
- Discussion : Q&A





Well known Topology to Study Attacks.

Study through Stories.

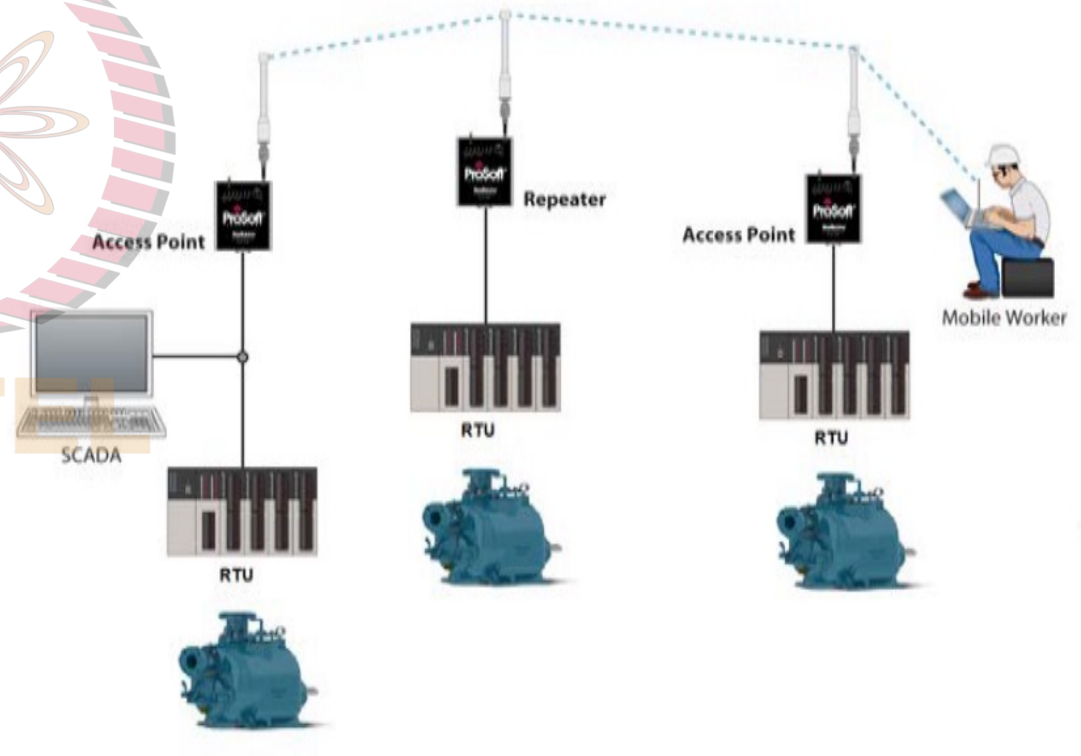
- Key Points to remember.
  - Threat Source.
  - Attack Motivation
  - Attack Scope
  - Attack Domain
  - Attack Mechanism
  - Attack Type
  - Targeted Principle.

Automotive Sector

- Daimler Chrysler – 2012 attacked by Cyber Actors to steal the Intellectual Property rights. Stole the credentials of the employee and used his access to login and copy the source code.
  - *A computer virus was detected on the network of an automanufacturer. Unknown attackers stole employees' IDs and encrypted passwords after planting a computer virus on the company's computer systems. The company waited a week to disclose the attack to allow time to investigate.*
  - *The company used their own security experts in addition to a third-party security consultant to investigate the attack. The company is still unsure where the attack came from. The company suspects that the hackers were attempting to steal intellectual property pertaining to the company's hybrid and electric vehicle drivetrains.*

Maroochy Shire Sewage Spill (2000)

- **Industrial Sector** - Energy Industry (E)
- **Threat Source** - Adversarial/Outsider.
- **Attack Motivation -** Revenge
- **Attack Scope -** Cyber-Physical
- **Attack Domain -** Software Communications
- **Attack Mechanism -** Subvert Access Control
- **Attack Type -** Active
- **Targeted Principle -** Confidentiality

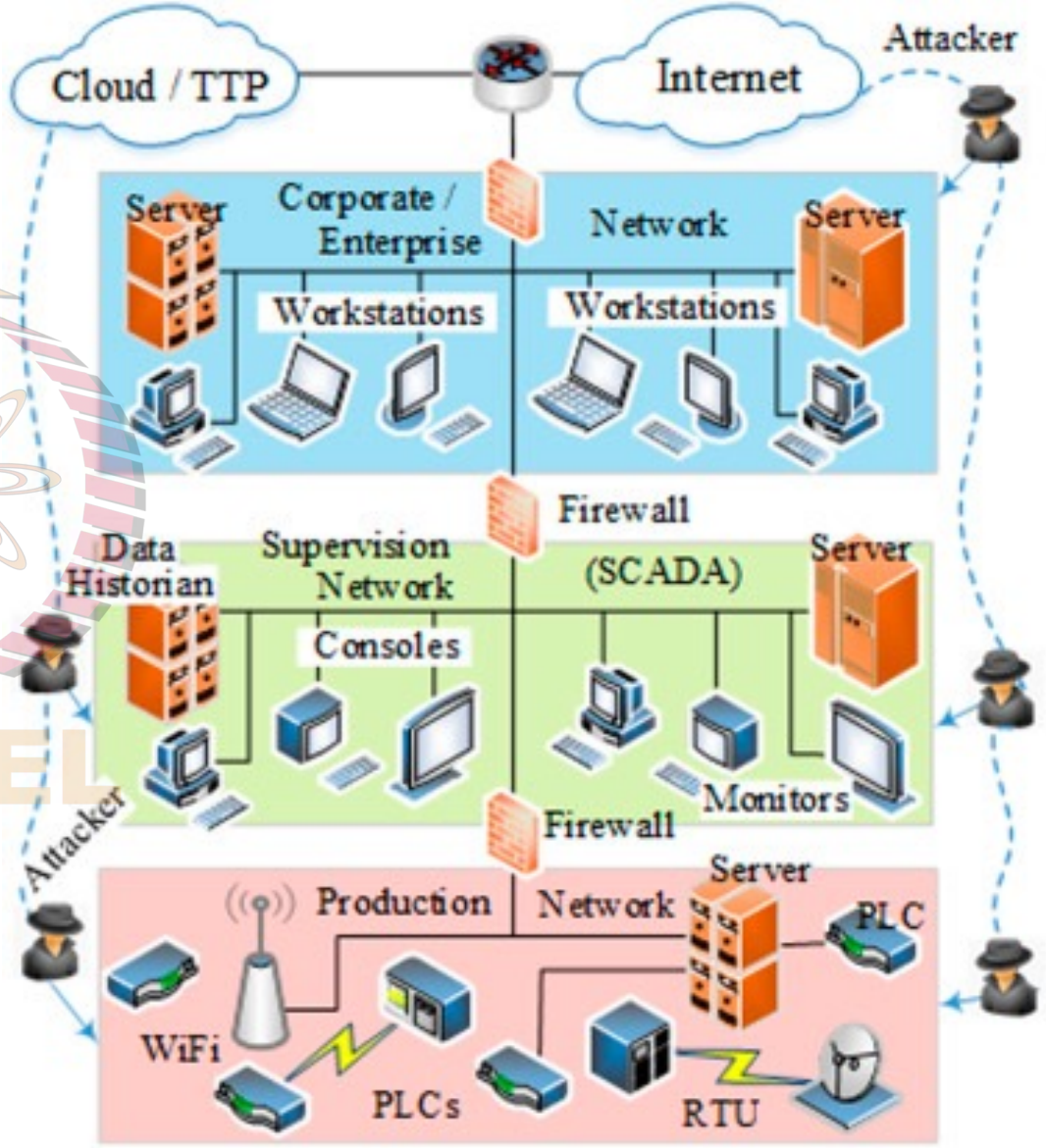


Kemuri Water Company Attack (2016)

- **Industrial Sector -** Energy Industry (E)
- **Threat Source -** Adversarial/ Nation - State
- **Attack Motivation -** Sabotage
- **Attack Scope -** Cyber-Physical
- **Attack Domain -** Software Social Engineering
- **Attack Mechanism -** Inject Unexcepted items
  Engage in Deceptive Interactions
- **Attack Type -** Active
- **Targeted Principle -** Integrity

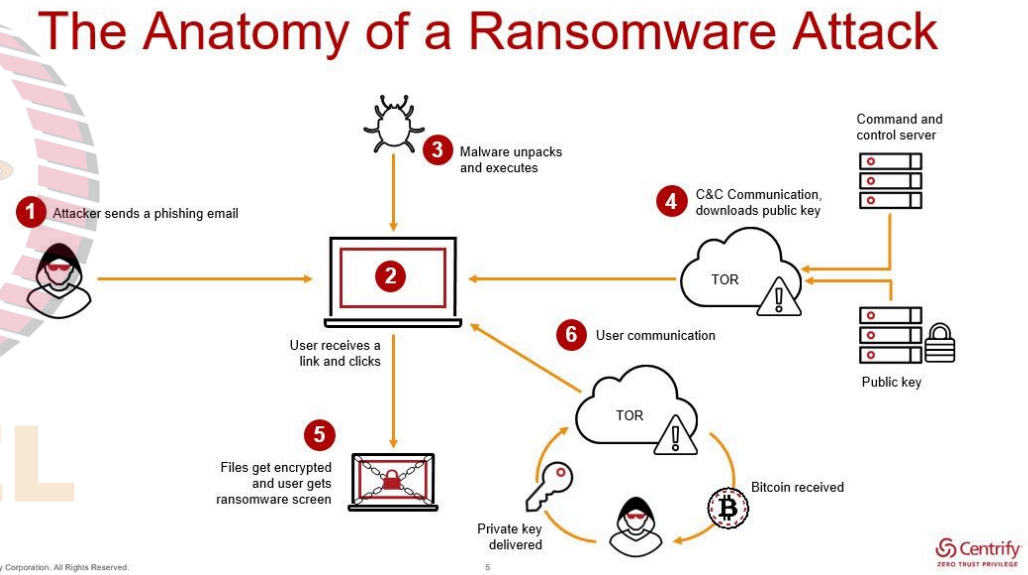
Crypto Mining on (SCADA)Attack - 2018

- **Industrial Sector -** Energy Industry (E)
- **Threat Source -** Adversarial/Group/Established
- **Attack Motivation -** Financial Gain
- **Attack Scope -** Cyber
- **Attack Domain -** Software
- **Attack Mechanism -** Inject Unexcepted Items
- **Attack Type -** Active
- **Targeted Principle -** Integrity



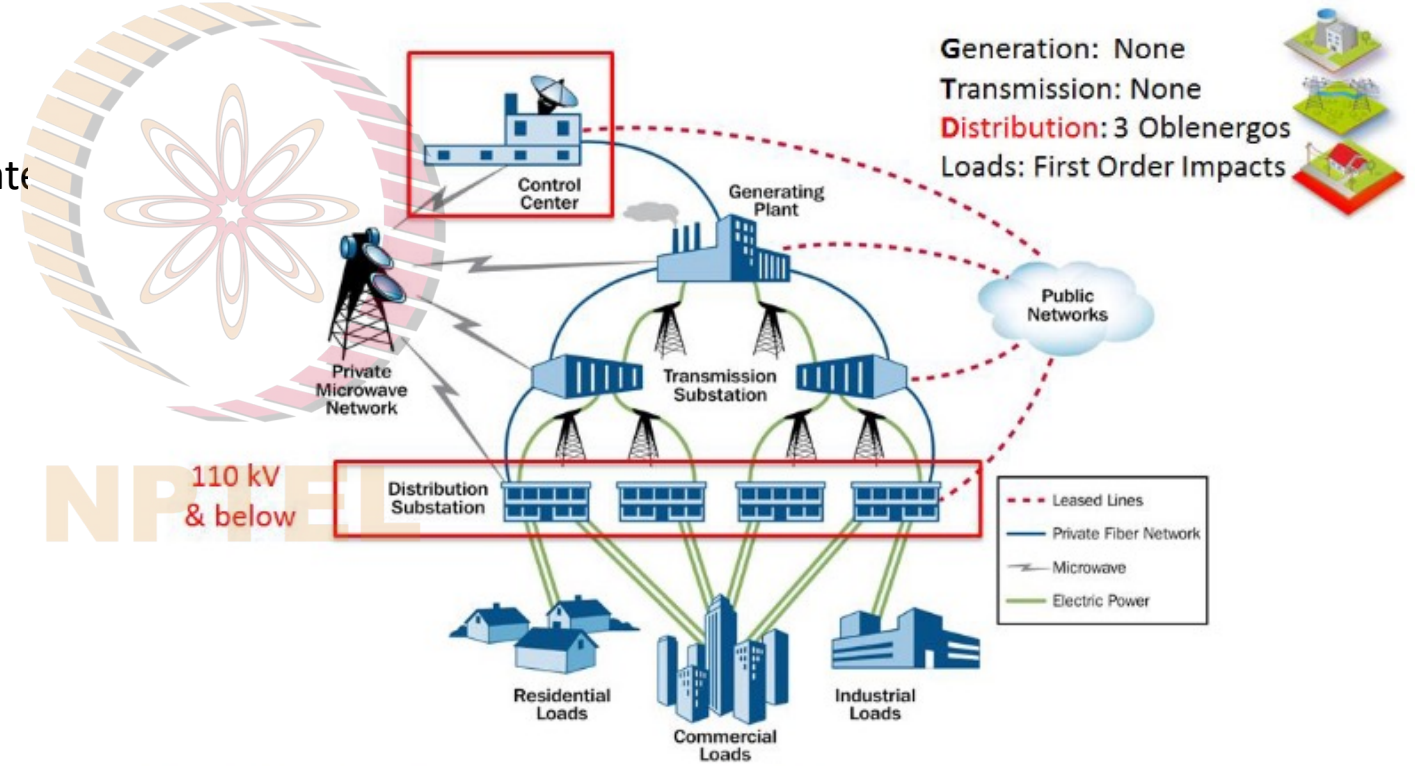
Riviera Beach Ransomware Atack(2019)

- **Industrial Sector -**Energy Industry (E)
- **Threat Source -** Adversarial/Group
- **Attack Motivation -** Financial Gain
- **Attack Scope -** Cyber
- **Attack Domain -** Software
- **Attack Mechanism -** Inject Unexcepted Items
- **Attack Type -** Active
- **Targeted Principle -** Availability



Ukrainian Power Grid Attack

- **Industrial Sector – Power Grid(D)**
- **Threat Source -** Adversarial/ Nation - State
- **Attack Motivation -** Sabotage
- **Attack Scope -** Cyber-Physical
- **Attack Domain -** Software/Hardware/ Communications/ Supply Chain
- **Attack Mechanism -** Manipulate System Resource
  Inject Unexcepted Items
- **Attack Type -** Active
- **Targeted Principle -** Integrity



Source: Modification to the DHS Energy Sector-Specific Plan 2010

Gas Compressor Station Attack (2013)

- **Industrial Sector -** Natural compressor stations (D)
- **Threat Source -** Adversarial/Outsider
- **Attack Motivation -** N/A
- **Attack Scope -** Cyber
- **Attack Domain -** Software
- **Attack Mechanism -** Employ Probabilistic Techniques
- **Attack Type -** Active
- **Targeted Principle -** Confidentiality

Home › Security Infrastructure

Cyber Attacks Targeted Key Components of Natural Gas Pipeline Systems

By Mike Lennon on July 01, 2013

Share Tweet Recommend 1 RSS

Attackers Used Brute Force Attacks Against Internet-Facing Controls Systems at Gas Compressor Stations

In its latest monthly report designed to promote preparedness, information sharing, and collaboration across infrastructure sectors, The Department of Homeland Security's ICS-CERT publicly revealed information on a series of attacks that targeted gas compressor station operators earlier this year.

According to ICS-CERT, on February 22, 2013, it received a report from a gas compressor station owner about an increase in brute force attempts to access its process control network.

Stuxnet (2009)

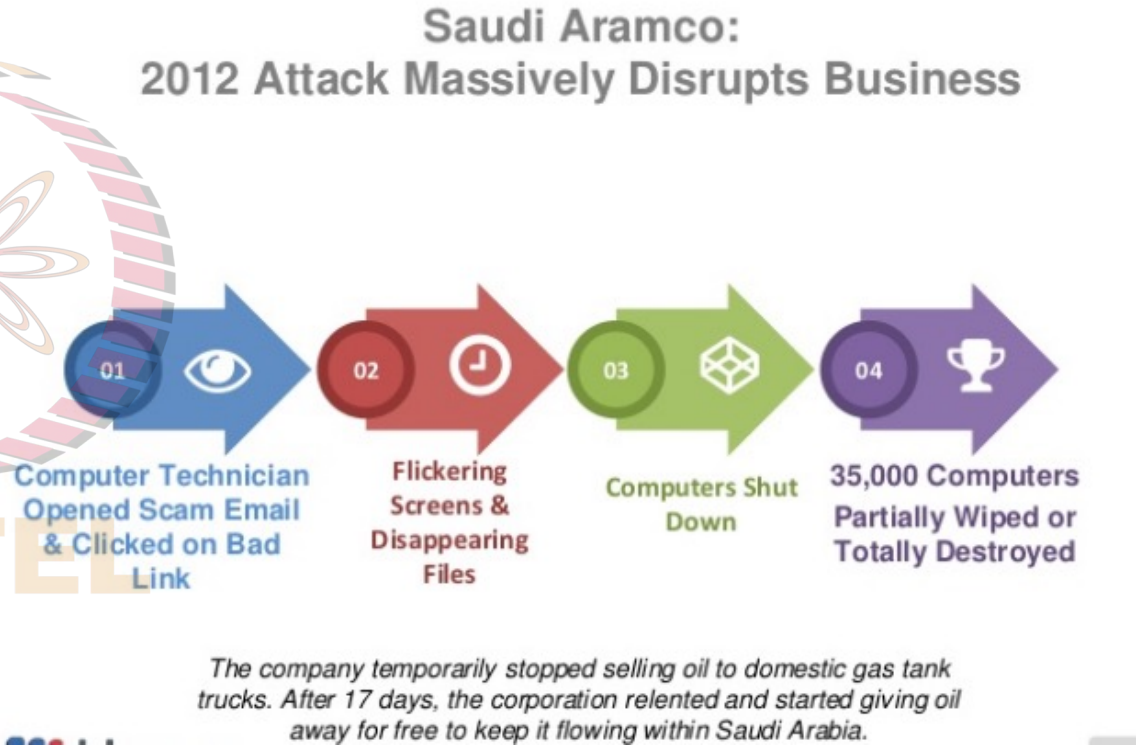
- **Industrial Sector –** Chemical Industry (C)
- **Threat Source -** Adversarial/ Nation - State
- **Attack Motivation -** Sabotage
- **Attack Scope -** Cyber-Physical
- **Attack Domain -** Software/Hardware /Communications
- **Attack Mechanism -** Engage in Deceptive Interactions/
  Manipulate System Resource/Inject Unexcepted items
- **Attack Type -**Active
- **Targeted Principle -** Integrity

Fukushima Daiichi Nuclear Disaster (2011)

- **Industrial Sector -** Chemical Industry (C)
- **Threat Source -** Environmental/ Natural Disaster
- **Attack Motivation -** N/A
- **Attack Scope -** Physical
- **Attack Domain -** N/A
- **Attack Mechanism -** N/A
- **Attack Type -** N/A
- **Targeted Principle -** N/A

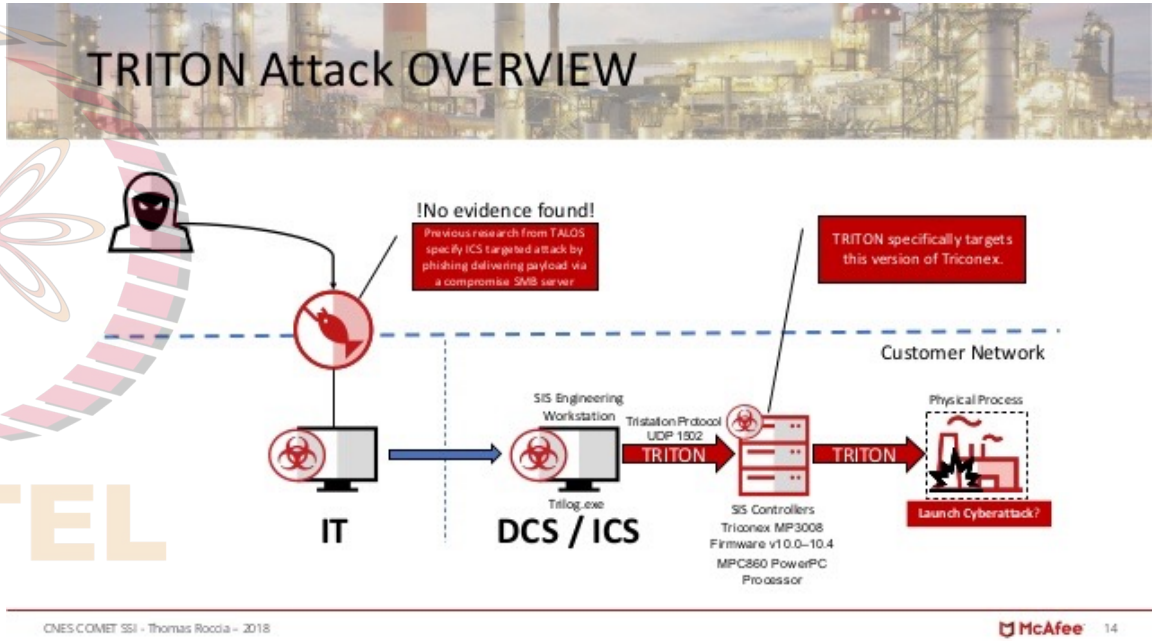
Saudi Aramco Attack (2012)

- **Industrial Sector –** Petroleume & Natural Gas (D)
- **Threat Source -** Adversarial/Group/Established
- **Attack Motivation -** Political reason
- **Attack Scope -** Cyber
- **Attack Domain -** Software Supply Chain
- **Attack Mechanism -** Manipulate Data Sturctures
  Subvert Access Control
- **Attack Type -** Active
- **Targeted Principle -** Integrity



TRITON Attack (2017)

- **Industrial Sector -** Chemical Industry (C)
- **Threat Source -** Adversarial/ Nation - State
- **Attack Motivation -** Sabotage
- **Attack Scope -** Cyber-Physical
- **Attack Domain -** Software /Hardware
- **Attack Mechanism -** Inject Unexcepted Items
  Manipulate System Resource
- **Attack Type -** Active
- **Targeted Principle -** Integrity



German Steel Mill attack (2014)

- **Industrial Sector -** Chemical Industry (C)
- **Threat Source -** Adversarial/Group/Copmetitor
- **Attack Motivation -** Theft
- **Attack Scope -** Cyber-Physical
- **Attack Domain -** Social Engineering Software
- **Attack Mechanism -** Inject Unexcepted Items Manipulate System Resource
- **Attack Type -** Active
- **Targeted Principle -** Integrity

Hack attack causes 'massive damage' at steel works

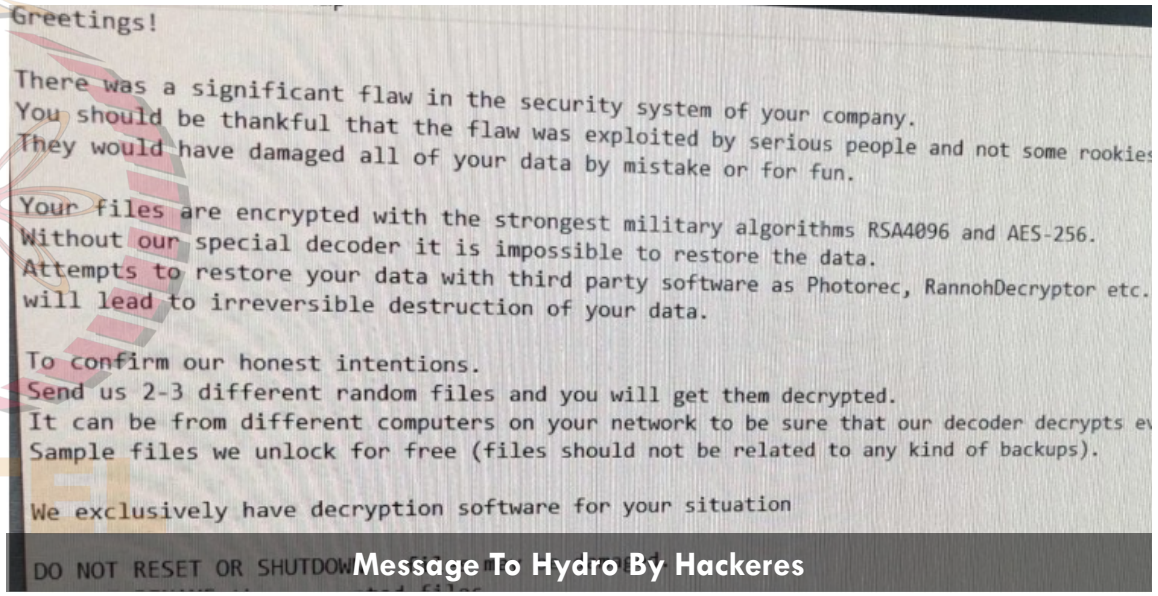
22 December 2014

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.

Norsk Hydro Ransomware Attack(2019)

- **Industrial Sector -** Chemical Industry (C)
- **Threat Source -** Adversarial/ Organization
- **Attack Motivation -** Reputation
- **Attack Scope -** Cyber
- **Attack Domain -** Software
- **Attack Mechanism -** Inject Unexcepted Items
- **Attack Type -** Active
- **Targeted Principle -** Availability



Message To Hydro By Hackeres

Godzilla Attack & Turn Back (2013)

- **Industrial Sector – Road Transport Sector**
- **Threat Source -** Adversarial/Individual
- **Attack Motivation -** Personal Entertainment
- **Attack Scope -** Cyber
- **Attack Domain -** Software
- **Attack Mechanism -** Subvert Access Control
- **Attack Type -** Active
- **Targeted Principle -** Integrity

CYBERSECURITY

Godzilla attacks? US warns of highway sign hack

PUBLISHED MON, JUN 9 2014·2:16 PM EDT | UPDATED MON, JUN 9 2014·3:43 PM EDT

REUTERS

SHARE

After hackers played several high-profile pranks with traffic signs, including warning San Francisco drivers of a Godzilla attack, the U.S. government advised operators of electronic highway signs to take "defensive measures" to tighten security.

TARGET Supplier Portal Attack (2012)

- **Industrial Sector –** Food Industry (D)
- **Threat Source -** Adversarial/Group/Established
- **Attack Motivation -** Financial Knowledge
- **Attack Scope -** Cyber
- **Attack Domain -** Software Social Engineering
- **Attack Mechanism -** Inject Unexcepted Items Subvert Access Controlls
- **Attack Type -** Active
- **Targeted Principle -** Confidentiality

Tridium Niagara Framework Attack (2012)

- **Industrial Sector –** Software Industry (D)
- **Threat Source -** Adversarial/Individual
- **Attack Motivation -** N/A
- **Attack Scope -** Cyber
- **Attack Domain -** Software
- **Attack Mechanism -** Abuse Existing Functionality
- **Attack Type -** Active
- **Targeted Principle -** Confidentiality

Investigations

Popular Niagara software vulnerable to hackers, Homeland Security warns

By Robert O'Harrow Jr.
July 13, 2012

The Department of Homeland Security on Friday warned that a popular system used by organizations around the world to manage millions of machines and devices over the Internet is vulnerable to attack from hackers.

The software system known as the Niagara Framework enables corporate, military, health-care and other users to remotely control or monitor medical devices, elevators, video cameras, security systems and a wide array of other sensitive operations.

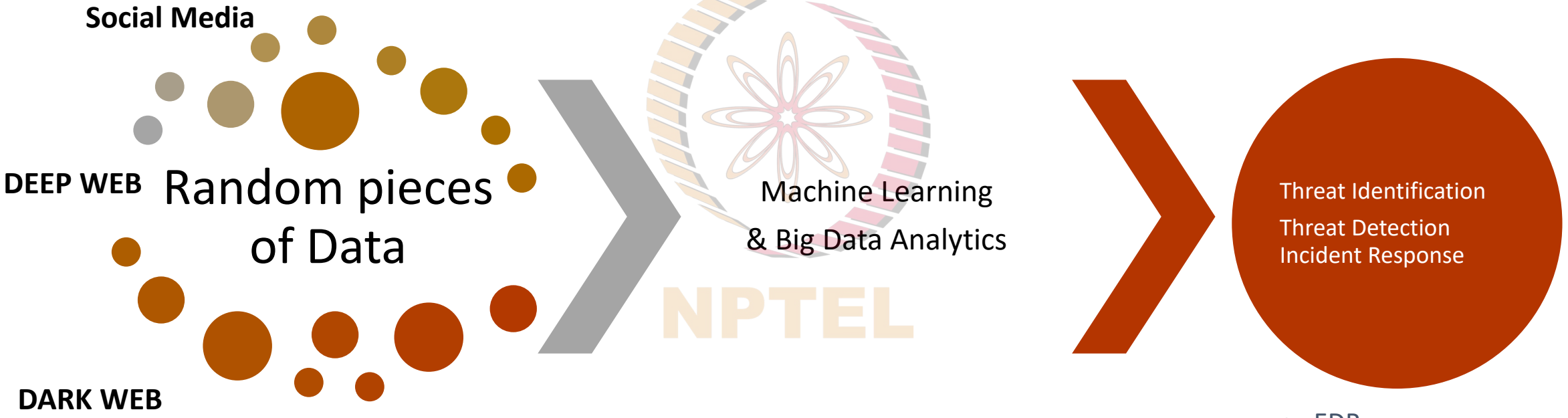
Introduction to Securing Institutions.

What is Threat Intelligence?

- “Details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.”

- Forrester

Threat Intel for organizations

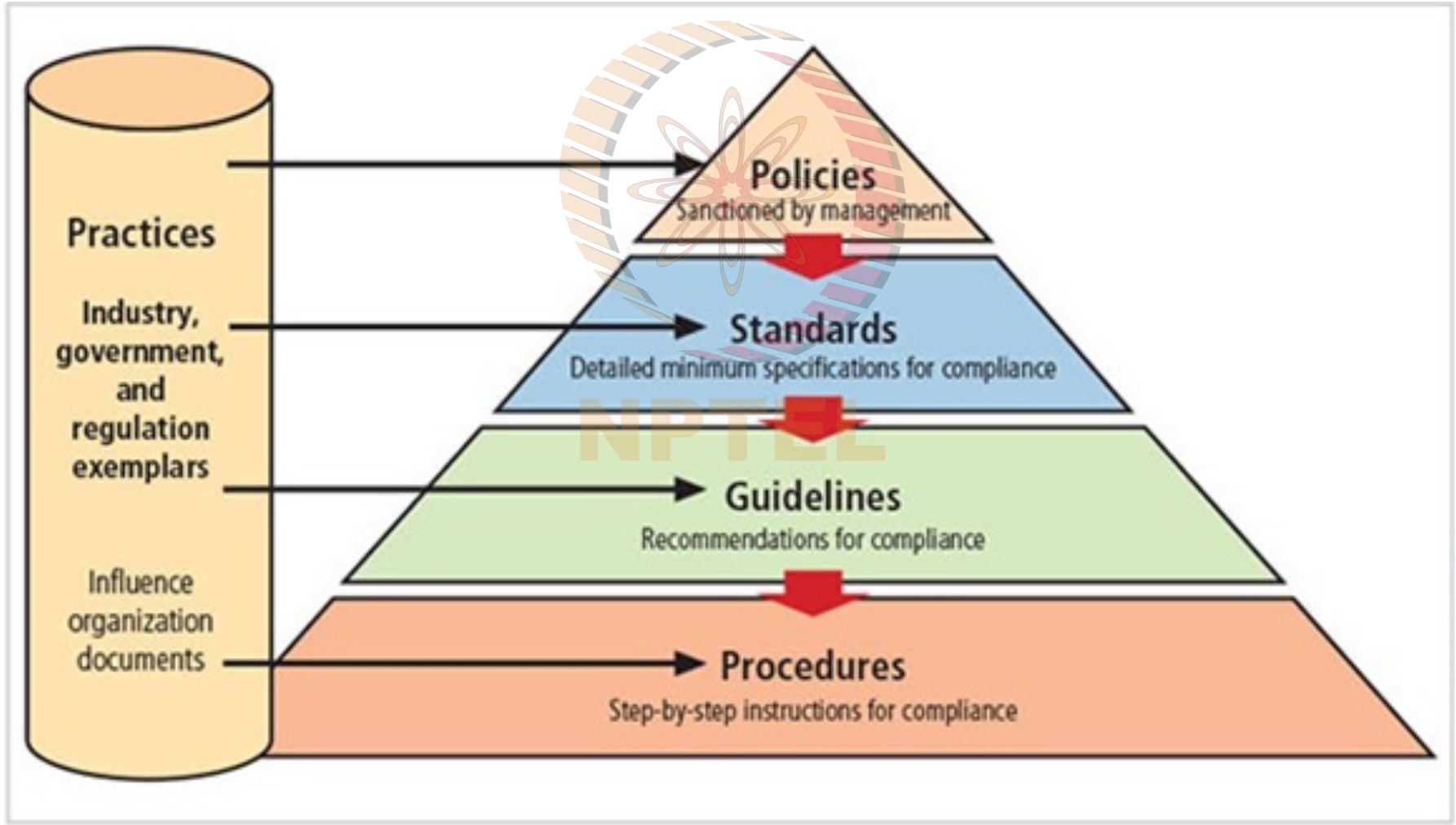


- Social Messaging Companies
- Telecom Companies
- Internet Service Providers
- Grocery & Pizza Providers.

- Log Aggregation, Triage, and Analysis
- Data Analytics
- Support for Threat Hunting

- EDR
- MDR
- XDR

Framework to study the Security of Org.



Challenges of CIIP

Integrity of Supply Chain.

Vendor Security Risk & Leakages

Boundary Protection – DMZ

Smart Monitoring - Use of Machine Learning – Anomaly detection etc.

Issues of Identification & Authentication.

Physical Access Control – Sabotage.

Interconnectedness – Risks.

Hardening of Systems – Limited Privilege.

Resource Allocation Caps.

Remote Access Permissions

Account Management

Discussion : Questions?

- Who is the Attacker?
  - Internal
  - External
- What is his Skill level?
  - Script Kiddies
  - Semiskilled
  - Highly Skilled
- What is his motive?
  - Espionage
  - Weakening & Demoralising organization.
- Which type of attack would be used for targeting your organization?
  - Focussed campaigns
  - Not Focussed campaigns
- Who is the Target?

Thanks & Questions.