

THE EVOLVING CYBER THREAT LANDSCAPE



Type of attacks



Example of respective attack

Supply Chain Attack



practices SolarWinds Attack

invades a network through a partner/ vendor having access to enterprise system and data

Occurs when an attacker

Root cause: Vendors with poor security

of end users by

Attacking a specific group

contaminating websites that are frequently visited by members of the group

DDoS Attack

Poor infrastructure and resource management of incoming traffic in victim's network

Root cause: Poor security controls for virtual machines and servers hosted by cloud companies

Installing a malicious Drive-by Attack script to download, install and program itself

the user



Root cause: Presence of insecure, outdated apps, browsers, or operating systems

into a device without

explicit permission from

Watering Hole Attack



Root cause: Vulnerabilities

DazzleSpy

in existing websites

A fraudulent practice of sending emails asserting to be from reputable companies in order to persuade individuals to reveal personal information

Root cause: Lack of security awareness





 \langle Root cause: Using same

usernames and passwords

across multiple services





RedAlpha

Phishing



Metamask



Malicious software designed to block access to a computer system in exchange of huge sum of money

LockBit

Root cause: Weak password and poor access management

Attackers attempting to exploit vulnerabilities found on application layer of the OSI model

Application Layer Attack

Root cause: Lack of

vulnerability (zero-day)

for malicious activities

Root cause: Presence of

vulnerability in system

in network



mechanism to fix loopholes and issues

Malware



Software designed to disrupt, damage, or gain unauthorized access to a computer system

Root cause: Lack of user awareness/vulnerable network service

Man in the Middle Attack



application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway

A fraudster positions

conversation between

himself in a

a user and an

Root cause: Poor information/data security

Exploitation of a Zero Day Attack previously unknown



Infosys CyberSecurity with the help of its suite of services, IPs (platforms) and Cyber Defense Centers assures digital trust to its clients. Infosys CyberSecurity service offerings encompass Identity and Access Management, Data Privacy and Protection, Vulnerability Management, Managed Security Services, Cyber Advisory Services, Governance, Risk & Compliance, Infrastructure Security, Threat Detection and Response, Cloud Security and Emerging Technologies to assure holistic security. Infosys Platform Powered Services Cyber Next (IP) delivered from its global Cyber Defense Centers assures round-the-clock monitoring, deep visibility, lifecycle management, automation and risk-based prioritization for proactive threat detection, analysis and response