Introduction to Cyber Security

Lab Sheet 3

**IT22151056**

**De Silva K.R.K.D**

Part 01

1. **China-Linked Bronze Starlight Group Targeting Gambling Sector with Cobalt Strike Beacons.**

* Vulnerabilities
* Adobe Creative Cloud, Microsoft Edge , and McAfee VirusScan executables.
* Exhibits overlaps with an intrusion set.
* Using .NET malware loader.
* Threats
* DLL hijacking
* Ransomware
* .NET malware
* Risks
* Financial loses
* Data breaches
* Assets
* Harmful DLLs for running programs and encrypted data files.
* Using compromised certificates to sign malicious software.
* Possible Controls
* Regularly update
* Analyze network traffics.
* Use strong access control.

# [Russian Hackers Use Zulip Chat App for Covert C&C in Diplomatic Phishing Attacks](https://thehackernews.com/2023/08/russian-hackers-use-zulip-chat-app-for.html).

# Vulnerabilities

# PDF documents with JavaScript code.

# Command and control communication.

# Threats

# Phishing attacks.

# Unauthorized access.

# Risks

# Data breach

# Disrupt operation and communication.

# Assets

# For C2 communication, chat programs are vital tool for threat actors.

* Possible Controls
* Regularly updates.
* Secure email

# [Cybercriminals Increasingly Using EvilProxy Phishing Kit to Target Executives](https://thehackernews.com/2023/08/cybercriminals-increasingly-using.html).

# Vulnerabilities

# Use Apple iCloud, Facebook like cloud environment.

# Threats

# Unauthorized access

# Steal bank information.

# Risks

# Financial losses

# Data losses

# Assets

# Unauthorized access for sensitive data.

# The Russian-origin phishing targets bank and credit information.

* Possible Controls

# Secure cloud accounts.

# Use web filters

# [New Attack Alert: Freeze[.]rs Injector Weaponized for XWorm Malware Attacks](https://thehackernews.com/2023/08/new-attack-alert-freezers-injector.html)

# Vulnerabilities

# Use ‘search-ms’ protocol to access an LNK file on remote server.

# Threats

# Unauthorized access

# Risks

# Sensitive data theft

# Unauthorized remote control.

# Assets

# Attackers target the victim’s cloud.

* Possible Controls
* Secure emails
* Use multi factor authentication

# [Researchers Expose Space Pirates' Cyber Campaign Across Russia and Serbia](https://thehackernews.com/2023/08/researchers-expose-space-pirate-cyber.html)

# Vulnerabilities

# Deed RAT AND Voidoor are use with undocumented malware that called Voidtools.

# Threats

# Unauthorized access.

# Data losses.

# Risks

# Data theft.

# Damage data

# Assets

# Sensitive data is at risk of compromise.

* Possible Controls
* Secure emails
* Analyze network traffic

**Part 02**

# China-Linked Bronze Starlight Group Targeting Gambling Sector with Cobalt Strike Beacons.

# China

# Adobe Creative cloud, Microsoft Edge and McAfee

# Not specified

# Compromised system

# Motivation -Theft of confidential information. They hope to achieve long term access and control.

# Sensitive data

# [Russian Hackers Use Zulip Chat App for Covert C&C in Diplomatic Phishing Attacks](https://thehackernews.com/2023/08/russian-hackers-use-zulip-chat-app-for.html).

# Ministries of foreign affairs of NATO-aligned.

# PDF documents.

# Duke malware

# Not specified

# Ministries of foreign affairs of NATO-aligned countries.

# Motivation - Intelligence gathering.

# Hope to achieve -