# Project: Laxman Rekha

Automating the Process of Defending and Investigation of Cyber Crimes

# Overview Of Presentation

01 | Identifying The Problem

02 | Proposed Solution

03 | Technical Details And Demo

04 | Conclusion

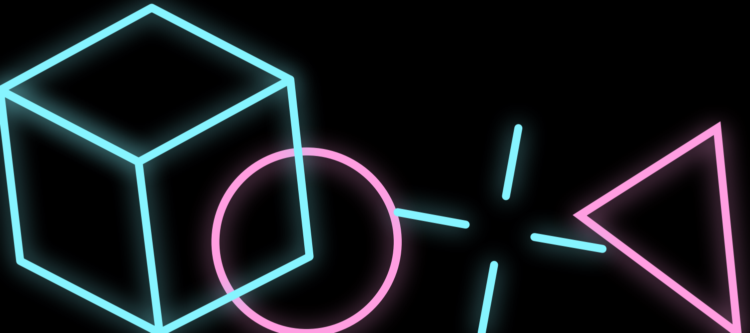
# 01

# Identifying the Problem

“India becomes the second-most targeted country for ransomware after surge in attacks over the last three months”

–Economic Times

October 07, 2020



For Reference: Click Here

# Ransomwares

Small and Medium Sized Businesses are often targeted by the threat actors as they are easy to attack and more affected by ransomware attacks.

These businesses don’t have a dedicated SOC team and have poor logging, backup and security policy. Thus once a ransomware is spread Incidence Response becomes very difficult for professionals.

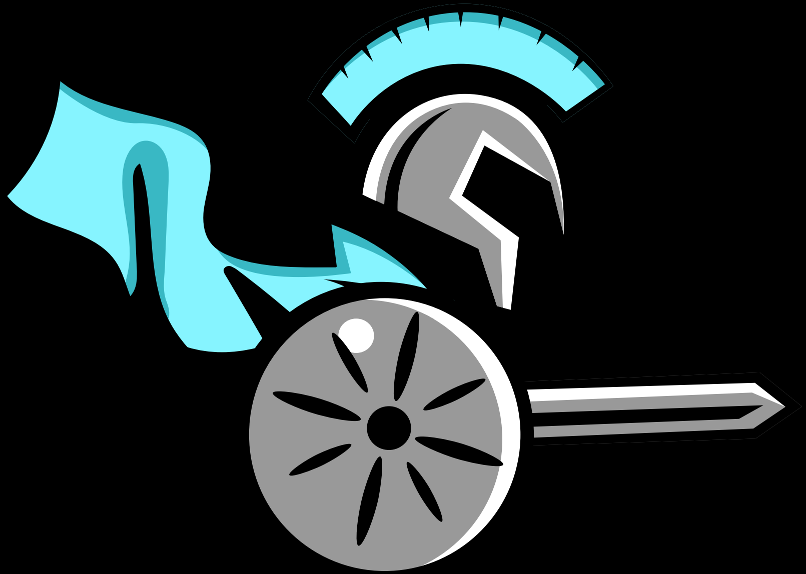
This eventually leads to them paying up the ransom and the threat actors are encouraged as an implicit action. Also due to poor Incident Response action the malware is never identified.

02

# Proposed Solution

# Project: Laxman Rekha

Automating the Process of Defending and Investigation of Cyber Crimes



# Basic Idea

The basic idea is that small to medium sized businesses that can’t afford a SOC team and have little to zero knowledge on securing their servers, can install this program in few clicks and the program will act as a guard on their servers and will do the following :

1. Harden the server from low level threats and automated botnets.
2. Scan the system for any misconfiguration that can lead to privilege escalation if a compromise occurs.
3. Fix the poor permission structure and password policy.
4. Enable regular logging and backups functionality.
5. Implement checks through out the filesystem to constantly monitor for any threats.
6. Once a threat is discovered it sends data over the network to a Delhi Police controlled server so they can get real-time graph for threats in the wild.

# How does it differ from an AntiVirus ?

The AntiVirus solutions are targeted towards personal usage and only scans for malicious file samples.

The Laxman Rekha adds protections, enables firewall rules and scans the file system for any clear text passwords and misconfigurations that can be used to escalate privileges on the box (if compromised).

Laxman Rekha is well suited for securing servers and enabling Monitoring features that will protect from ransomwares and will help professionals in investigation if one happens.

Once a threat is found the project alerts the user and the government controlled server that a new malware signature is in wild.

# 03

# Technical Details And Demo

# Work Flow of the Program

Since the idea is to make an easy to use utility to secure remote servers, the language of choice for main driver was Go.

Go is used to create main driver of the code that will run main host of the user and use ssh credentials to login into the server.

After the setup is finished the program will run the system like service and monitor for threats in real-time.

Once a threat is discovered it sends data over the network to a Delhi Police controlled server so they can get real-time graph for threats in the wild.

This will allow us to have real-time idea of which malware is affecting the most servers in the wild.

## GoLang

Main Driver
Function

## Perl

Automating Setup
on linux Hosts

```
888                                                        8888888b.          888      888
888                                                        888   Y88b         888      888
888                                                        888    888         888      888
888  8888b.  888  888 88888b.d88b.   8888b.  88888b.       888   d88P .d88b.  888  888 88888b.   8888b.
888     "88b  Y8bd8P' 888 "888 "88b     "88b 888 "88b      8888888P" d8P  Y8b 888 .88P 888 "88b     "88b
888 .d888888   X88K   888  888  888 .d888888 888  888      888 T88b  88888888 888888K  888  888 .d888888
888 888  888 .d8""8b. 888  888  888 888  888 888  888      888  T88b Y8b.     888 "88b 888  888 888  888
888 "Y888888 888  888 888  888  888 "Y888888 888  888      888   T88b "Y8888  888  888 888  888 "Y888888
```

# Demo

# 04

# Conclusion

# Conclusion

With the help of Laxman Rekha we were able to :-

1. Stop threat actors from going after easy targets.
2. Since we are able harden the servers from common attacks; botnet based attacks will be stopped to a great extend.
3. This could be a great open source project to help improve cybersecurity demands of businesses with no budget for SOC.
4. Government will have better grasp on ground reality of how ransomware attacks are going around.

# Thank You