Methodology

The study will be conducted through an extensive literature review, obtaining information across various organizations to evaluate what steps are taken to secure the valuable data in cyberspace.

Assumptions

The critical infrastructure this paper will focus on is the Banking and Finance sector. The main objective of the cyber weapon/malware will be to cripple the finance and banking sectors of the nation for the longest time possible to cause maximum damage to the nation's economy. The name of the malware is assumed to be **Kaos.**

Kaos – A brief overview

Kaos is a new type of cyber weapon that the world has never seen before. Developed as a joint venture between intelligence agencies, and militaries of China and Pakistan. Kaos targets the banking and financial services and infrastructure of the target nation with the primary goal to cripple and decimate the economy of the target nation.

Kaos was developed specifically to target Indian banking and finance infrastructure. Its nature is polymorphic. Therefore, it can avoid detection from antivirus softwares with ease. Moreover, this is a completely new type of malware that the world has never seen before thus information security firms and vendors do not know its behavior and no prior signature of this malware is available which may aid in its detection.

Kaos was developed specifically keeping in mind the information security practices that are being followed in India. Kaos also utilizes zero-day vulnerabilities and known vulnerabilities that aren't patched.

Goals

- Threaten the integrity of financial data either by encrypting it or damaging it permanently.
- Steal the user data.
- Stall the transaction processes across the country by attacking ATM networks and UPI servers.
- Stay undetected for as long as possible to cause damage to economy.
- Spread further in share market networks and decimate the functioning and integrity of the share market data pushing investors into chaos.

Attack Vectors

- **Social Engineering:-** Developers of the Kaos did extensive research in understanding the information security practices that are being followed in India. They found out that the majority of people in India are not aware of proper information security practices, especially the older people. Social Engineering attacks like phishing, and spear-phishing are used to easily get access into internal networks either by stealing credentials of the higher ups in the banking and finance sector or by sending the payload through an infected mail, attachment, file etc.
- **Inside Job:-** Since the nation-states are involved in the attack. They can utilize intelligence agencies, spies, and their assets in India to either bribe the higher-ups in the banking and finance sector to gain access or by blackmailing the important employees to gain access to the internal networks. They can accomplish this by forcing the employee to plug a USB infected with the malware into the system which is present in the network or by forcing the employees to leak the credentials which can be used to gain access.

Attack Scenario

After getting initial access into the internal networks, Kaos will try to spread into as many systems as possible which are present in the network. Since the internal networks are isolated and each bank has its own network, attackers can inject the malware in the networks of multiple banks by utilizing the aforementioned attack vectors. After getting into the network Kaos will stay dormant for a pre-determined amount of time, say 4 months so that it can spread to as much systems as possible in the network and also giving the time to enemy in physical world to inject the malware into as much networks as possible.

After its dormancy period is over it will begin its attack. Since now it has spread over a large number of systems in the network, possibly in all systems. The main goal is to cause maximum damage in a short period, the longer it stays undetected the more the damage.

It will first try to disrupt the services of banks to bring nationwide outage to online transactions then it will try to disrupt the ATM machines since its spread all over the internal network. Then it will attempt to damage the data present in databases of the banks either by encrypting it with complex encryption algorithms like RSA, AES-256 or it can even use a custom encryption algorithm which is not known to the security community or by permanently deleting the data. Attackers can also inject the malwares into backup facilities thus ensuring the complete loss of data and maximum damage.

It can be observed here that the initial phase of Kaos was stealthy but its attack phase focuses on dealing maximum damage in short amount of time while also managing to stay undetected for as much long as possible. The way it deals maximum damage is by destroying financial data and its backup.

Cyber Deterrence Challenges

- Since the attackers are relying heavily on social engineering techniques, it's pretty evident that they are exploiting human behavior and psychology. Human errors although may seem simple as compared to technical errors but are the most difficult to mitigate. Human behavior and nature are unpredictable. A seasoned security analyst may handle technical aspects of the malware very well by researching it thoroughly, identifying patterns, and developing patches to fix the vulnerabilities but predicting human behavior is something else entirely. Humans become very unpredictable under mental stress. Attackers can readily exploit this, since nation-states are involved which means enemy intelligence agencies are also in play here and they can easily honeytrap, extort or blackmail high-ranking employees in the banking sectors, e.g. by kidnapping a family member of the employees and then blackmailing them to give in the confidential security information, again this is one of many possibilities since it's difficult to determine how a person would react in such situations, especially a normal person who is not trained to handle extreme mental stress and pressure.
- Most of the cyber-attacks if not all can be prevented or slowed down if only proper security practices are implemented. But unfortunately in India, a vast majority of the population still lacks the proper technical knowledge of cybersecurity. The attackers kept in mind this aspect because in India still, many systems run outdated and vulnerable software and the staff and employees also lack proper knowledge of security practices. If only the users are aware of what they are doing and realize the consequences of their actions, it can make the jobs of people working in Infosec a lot easier, but the reality is often disappointing.
- The security team responsible for defending against the attack must be properly and rigorously trained to handle these situations. These situations

are no different than the battle going in on the frontlines. Just in case on a battlefield a wrong decision or no decision at all can lead to severe consequences, the same can happen in a cyberwarfare scenario.

Legal and Treaty Assumptions

Hostile nation-states involved in the attack are China and Pakistan. These nation-states were identified based on inputs provided by Indian Intelligence Agencies. India can ask for assistance from allied nations such as US and Russia. Limited assistance is expected from the US as it rarely shares its resources with other nations but since this cyberweapon is unique, the US will probably want to get its hand on Kaos to analyze it and use its technology for their purposes. Russia, on the other hand, has very strong diplomatic relations with India and Russia's expertise in cyber warfare can help India greatly. But Russia also has strong ties with China so expecting full support from Russia seems impractical. Russia will try to remain neutral whereas countries like the US, Japan, France, UK will take India's side but they won't push themselves into a cyber war. The situation will be very likely similar to the Russia-Ukraine war. But cyber warfare tends to be covert in nature contrary to conventional war where allegiance of the countries is very clear. This can blur the line between allegiance and hostility.

Solution Architecture

The solution will focus on the technical and non-technical aspects.

Non-Technical

- As previously seen, attackers gained initial access through social engineering attacks. Attackers took their time in analyzing their targets, they studied their information security practices and chose their targets. Non-technical aspects such as human errors and human behavior are difficult to predict and protect against.

- Proper security and background checks should be done on the employees working in critical national infrastructures such as banking and finance. Employees must be taught proper security practices and must possess requisite technical knowledge.
- To ensure the technical literacy of the employees, training, and workshops should be held at regular intervals to make them aware of the rising cybersecurity threats.
- They must be made aware of the consequences of their actions, consequences may get exacerbated since these are the critical national infrastructures, therefore the authorities and government must ensure that they properly train the employees and staff to handle the situations when they are attack. Well, if they implement best security practices, chances of attacks gets reduced greatly.

Technical

- Perimeter security of the buildings of critical infrastructures must be tight so that any unauthorized access to the buildings is prevented. Perimeters must be made secure with proper fencing and surveillance through CCTV cameras and regular guard patrols must be maintained. Any suspicious person and activity observed must be taken care of immediately.
- The internal networks must be made secure by implementing proper IDS and IPS configurations. Suspicious traffic and packets must be kept in check, and proper firewall configurations are also important. Deep packet inspection must be performed on suspicious-looking packets. Any suspicious behavior in the network, even though it may seem like a false positive must be kept under scrutiny.
- In case of a possible attack, collaboration and coordination with intelligence agencies are important. Advanced intelligence inputs and warnings from intelligence agencies can help in preparing for the attack beforehand.

- During the course of an attack, the availability of services must be of top priority. The infrastructure must not go down for a long period of time. Backup facilities should immediately come into play to maintain availability of the services.
- Backup facilities and data storages must be isolated from the infected network if they aren't then they should be isolated immediately to prevent further infection.
- The Blue Team and Incident Response Team must quickly act upon a plan and try to minimize the effects of the attack. They must analyze the attack patterns of the malware and the processes the malware targets.
- Automated and AI-based tools can greatly help in analyzing the malware. They can detonate the malware in an isolated environment to observe its behavior.
- Zero-Trust policy must be implemented at all levels of the infrastructure. Especially, if the organization supports BYOD (Bring Your Own Device).
- After the availability of services is ensured, the threat still persists because until this moment thousands of systems are infected. A dedicated team of reverse engineers must work round the clock to analyze what the malware does and how it is able to do.
- Defense Ministry should be made aware of the situation and a strategy for retaliation must be enacted after the clearance from the ministry.

Benchmarks for Success

- The defense strategy would be considered successful if it manages to fend off the attack in such a manner that critical functioning and processes are not affected for a longer duration of time. The critical services must be kept up and running during the attack. If they are down then they must be brought back to their full operational capability as soon as possible.
- During a cyber-attack the MTTD (Mean Time to Detect), MTTR (Mean Time to Response) and MTTC (Mean Time to Contain) must be as

minimum as possible. The cyber weapon should not reach its maximum operational capability, it must be stopped before it does what it was intended to do.

- In case of an offensive cyber warfare operation, the offensive would be considered a success if the attack successfully manages to take down enemies' critical infrastructures for extended amount of time and reach its full operational capability while manages to remain in the systems and infrastructure as long as possible, avoiding detection. In case of overt operations, such as DDoS attacks, the source of the attacks should not be easily traceable (use of proxy chains can make tracing a tedious task).

References

- Polymorphic malware:- https://digitalguardian.com/blog/what-polymorphic-malware-definition-and-best-practices-defending-against-polymorphic-malware
- Zero-Trust policy :- https://www2.deloitte.com/nl/nl/pages/financial-services/articles/zero-trust-never-trust-always-verify-tech-trends-banking.html
- Benchmarks for successful cyber offensive:- https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf
- IDS and IPS :- https://www.varonis.com/blog/ids-vs-ips
- Availability:- https://www.geeksforgeeks.org/availability-in-information-security/
- Social Engineering :- https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html https://www.itgovernance.co.uk/social-engineering-attacks