Introducing the Insider Threat Kill Chain

Key Themes

- The traditional Kill Chain model needs to be updated due to the new cyber landscape
- A new Kill Chain for detection of The Insider Threat needs to be proposed
- By understanding each stage of The Insider Kill Chain, you can deploy the correct policies and technical solutions to help identify and stop an Insider Threat before they are successful

Introduction:

The Insider Threat has become a phrase that most IT managers and CISOs have come to know due to the rise in high profile incidents in the press, and the fact that this form of threat is just so difficult to identify and deal with effectively. This is because insider threats are influenced by culture, technical and behavioural issues in an organisation and must be tackled by the implementation of policies, procedure and technologies that must have the support of the board and senior management in order to be effective.

As an information security professional, you may have been asked to implement an insider threat mitigation programme and if you're lucky you might have been given a budget to do so. With or without a budget, it's often hard to know where to begin to deploy policies and technologies to help you gain the necessary insights into user behaviour.

The purpose of this document is to present a framework for thinking about the critical stages an insider goes through in order to steal information from your company. This framework is based on the experiences we have with working with customers to help them identify potential areas of weakness in their organisation. We have decided to base it on the Cyber Kill Chain, first presented by Lockheed Martin, as it is a widely recognised, well-known, and has been proven to be useful in helping prevent traditional security incidents. By breaking the stages of an insider attack into steps, you can best assess and identify the existing or new policies, procedures or technologies that need to be deployed in order to detect and stop an Insider to prevent your organisation from suffering from the business impact from this form of data breach.

The Cyber Kill Chain

Lockheed Martin coined the term 'Cyber Kill Chain' to describe the most common sequence of events observed in the majority of cyber-attacks on organisations. They defined the stages in the Kill Chain as:

- Reconnaissance
- Weaponisation
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

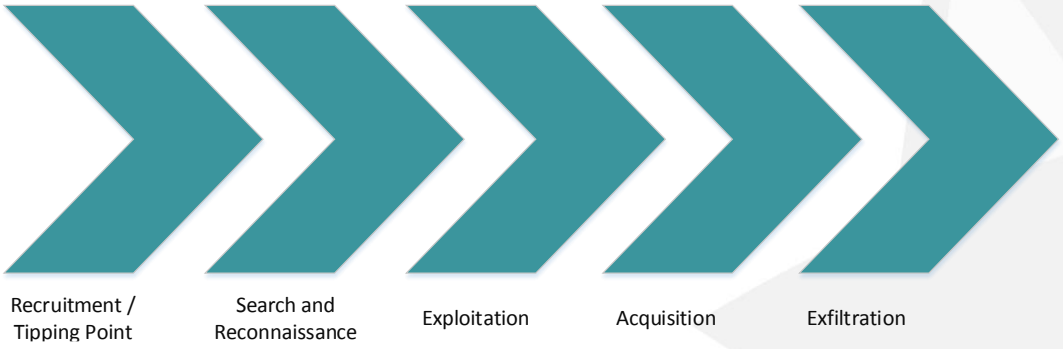
The classic Kill Chain is typically representative of an external attacker attempting to gain entry to an organisation through a perimeter. All of the steps are necessary in order for an attacker to successfully compromise an organisation. If one of these steps is interrupted, or the chain is 'broken', then the adversary would fail in their attempt. Therefore, it is necessary to have policies, processes and the capability to identify whether someone was attempting the stages of the Kill Chain in your organisation.

The Insider Threat Kill Chain

ZoneFox has worked with partners and customers to help them identify the Kill Chain that best represents the insider threat. As a result we have come to recognise that we need to define an additional Kill Chain that doesn't just focus on external attackers as there's risk from insiders whether they are your employees, contractors or partners. These are the people that have access to your systems and data and yet they are often partly overlooked when considering where data loss may occur. As a result, we've recognised that an Insider does not follow the traditional Kill Chain.

Based on our experience, the Insider Threat Kill Chain would look like this:

- Recruitment or 'Tipping Point'
- Search and Reconnaissance
- Data Acquisition
- Exfiltration of Data



Recruitment or 'Tipping Point'

There are many reasons for someone inside your organisation to decide to maliciously steal information from your organisation. Existing employees can reach a 'tipping point' where they have been coerced or tempted by an external party to steal for financial gain, or have a grudge against the organisation. The Insider Threat can also manifest in the form of contractors and service providers, or business partners.

Search and Reconnaissance

Once an insider is within your organisation, or they have reached the 'Tipping Point' their initial aim will be to search for valuable data on their own system or to find systems which could them access to valuable data.

Exploitation

When the insider has identified systems that contain valuable data, they must gain access to the data. This may involve using their existing credentials and systems, or gaining access to new software, credentials and methods of accessing your valuable data.

Acquisition

Once valuable data has been identified and accessed, an insider will aim to collect extracts of this data in a central location or series of locations prior to removing the data.

Exfiltration

The data has been identified, accessed, prepared for removal and the final stage in the data theft is to exfiltrate the acquired data.

All stages of this Kill Chain are difficult to identify due to the fact that internal employees are typically granted access to critical data, and are given permission to install applications which may be used to identify and acquire data for exfiltration. Combine that with the rise in shadow IT, and you may have a number of blind spots within your organisation.

The Insider Threat Kill Chain in Action

The following case study is based on the work the ZoneFox team undertook in a globally recognised engineering firm. During a deployment, ZoneFox discovered an employee accessing and removing highly valuable intellectual property, estimated to be worth £10m, from the computer systems of the firm. Each of the stages that the employee undertook is mapped into the corresponding Insider Threat Kill Chain stage.

Stage	Details of Malicious Activity
Recruitment/Tipping Point	Engineer A hands in his resignation. Unknown to the ZoneFox team at the time, he was due to leave for a competitor.
Search and Reconnaissance	Over a period of time, Engineer A went to a number of network shares which held files and data for different divisions within the organisation. The Engineer explored a number of different areas by browsing directories and opening files.
Exploitation	In this case there was no sophisticated exploit other than the fact that the organisation did not have critical and sensitive areas of their network controlled with the correct levels of permission. Where organisations require open and free access to data, or have not implemented basic access control, this is a common example.

Acquisition	Once Engineer A had identified the information he wanted to steal, he downloaded a piece of software designed to create backups. He installed this on his machine and configured it to retrieve the necessary files from network locations to consolidate them in a single file. Once it had performed its initial backup, he was clever enough to configure it to perform an incremental backup, which means that if the files in the locations change, or new ones are added, the backup software would only add the new or modified content.
Exfiltration	Once Engineer A was ready, he unplugged his endpoint from the network, and loaded the backup file onto a USB thumb drive.

Summary

Insider Threats are typically not sophisticated hackers trying to break into your network. They usually don't use complex malware or cracking tools to gain access to your most vital information. This is because they can typically traverse and access information with ease as they are internal to your organisation. Unless you implement sufficient controls and auditing capabilities at each stage of the Insider Threat Kill chain, your organisation will not be able to understand the key behaviours that will end in current or ex-employees, partners, or contractors walking out the door with your business critical documents.

About ZoneFox

ZoneFox is a highly innovative Endpoint Monitoring & Threat Detection solution that helps our customers protect their business-critical assets: data and intellectual property (IP) from malicious and accidental insider threats. ZoneFox has a proven track record of protecting reputation, sales revenue, and competitive advantage by providing next generation data monitoring, security analytics and endpoint security, enabling:

- Policy compliance monitoring
- Data and Intellectual Property Protection.
- Protective monitoring of user risk