Cyber Kill Chain

The cyber kill chain is the name given to a framework which is used to analyse cyber-attacks on a step by step basis in an effort to understand how each step was achieved and how this in turn led on to the next step. The overall aim of any cyber kill chain is to equip the parties responsible with the information needed to be better able to understand the nature of the cybercrime threat and to be better equipped to recognise and combat specific problems such as security breaches, ransomware and advanced persistent threat (APT).

The concept was first devised by Lockheed Martin and – like the red and blue team technique discussed in a previous blog post – was based on a military model devised to prepare combatants to identify targets, prepare to attack and then engage and destroy.

The stages of the cyber kill chain cover everything from the reconnaissance which often precedes a malware attack through to lateral movement across a network once access has been achieved and finally on to the data exfiltration which is the end game of most cyber-attacks. Although designed around the threat of external threats the kill chain can also deal with activities involved in an insider attack, and the more advanced iterations of the framework will be tweaked to make allowances for the growing awareness of the extent and severity of insider action.

The stages of the cyber kill chain break down as follows:

Reconnaissance

This involves the attacker analysing the target, looking for the information which might uncover vulnerabilities in the system or weak points in the security. It often involves gathering publicly available information such as email addresses and other details in order to build a profile of employees through factors such as their online presence, position within the organisation and area of expertise. Reconnaissance is also used to build a picture of the infrastructure of the target, including its software, security tools and devices. It can be carried out through access to open source intelligence and general research or by gaining unauthorised access to the resources of the organisation.

An example of this kind of activity was uncovered in April of this year, when anonymous hackers infiltrated organisation such as the WHO and the Bill gates Foundation in order to harvest almost 25,000 email addresses and passwords which were subsequently posted online. Once online, the details were used to facilitate hacking and other forms of cyber-attack.

Intrusion

Intrusion is the point at which the cyber-criminals leverage the information gleaned during reconnaissance in order to gain access to the systems. Having spotted vulnerabilities in the defences, the hackers will use tools like spyware, adware and ransomware in order to gain entry. This is also the delivery stage of the attack and could be facilitated by tools such as a phishing email, a link to a compromised website or a user logging on to a Wi-Fi system (such as one offered free of charge in a public place) which doesn't have suitably rigorous security measures in place. This is the point at which the attackers gain entry to the systems being targeted.

Exploitation

Being present in a system is one thing, but hackers want to be able to exploit their illegal entry as fully as possible. The process of exploitation – which basically means ensuring that they get to enjoy access which is as wide and potentially damaging as possible – might involve installing tools, modifying security certificates and creating new script files.

An example of real world exploitation – one which underlines the growing attack surface opened up by the internet of things – happened in March of this year, when hackers targeted the Zyxel Communication Corp, a company behind around 100 million hardware devices globally. The hackers managed to install malware known as Mukashi onto Zyxel hardware. Once in place, Mukashi scans the internet looking for Internet of Things (IoT) devices which are often vulnerable to attack, having been left with factory default security settings or commonly used passwords. Once the IoT systems have been infected by Mukashi they connect to a control server which enables actions such as downloading new software or launching distributed denial of service (DDoS) attacks.

Privilege Escalation

Once they've established themselves within a system, hackers will seek to escalate the privileges they enjoy within that system in order to create new permissions and access further data. The techniques employed to make this happen might include targeting vulnerable passwords, exploiting zero day vulnerabilities (the name given to a vulnerability in a system or device which has been spotted but does not yet have a patch or update) or launching brute force attacks. With escalated privilege the hackers will be in a position to try to extract credentials, modify configuration files and change permissions.

Lateral Movement

Having gained full access to one system, hackers will begin moving laterally from system to system and across accounts with the intention of gaining ever greater access and uncovering more assets. Lateral movement of this kind also represents an advanced data mining operation, with the hackers moving through an IT infrastructure seeking out critical data, sensitive information, further admin access and assets such as email servers.

Obfuscation / Anti-forensics

Up to this stage any cyber-attack has merely been an exercise in gaining and then exploiting access to a system and/or systems. Obfuscation marks the point at which the hackers begin taking steps to cover their tracks and mask their activity. This is done on the assumption that the security systems in place might by now be expected to be alerted, and so the aim is to mask activity and plant false trails in order to slow down or confuse any investigations. Methods used to do this might include clearing logs, wiping files and metadata, and using techniques such as overwriting false timestamps and modifying other information to create the information that the data in question is still untouched and safe.

Denial of Service

The penultimate phase of any attack involves a serious escalation. Until now the hackers have been attempting to move stealthily and silently through the system, but at this stage they take action which can easily be identified because the intention is simply to lock the

legitimate users out of the system. This is achieved by launching a denial of service (DoS) attack which floods the system, causing it to crash and suspend access for anyone wishing to track and block the attack in progress. By now the administrators of the site may well be aware that an attack is underway, but will be unable to do anything about it.

Exfiltration

The exfiltration stage is the end game of the attack and the ultimate point of launching it in the first place. Having discovered and gathered the data they need, the attackers will take it away with them, copying, transferring or moving it to a controlled location. Once they've done this they can do as they please with the information, from selling it on eBay to sending it to Wikileaks or ransoming it back to the original owners.

Sometimes the exfiltration happens over an extended period and isn't preceded by a denial of service to set alarm bells ringing. This was demonstrated in May this year when an APT group targeted a range of organisations in Central Asia including a telecommunications company, a gas company, and a governmental institution. Having infiltrated the networks of these organisations they planted backdoors which enabled them to quietly extract information over a prolonged period. A cyber kill chain analysis of the attack identified it as making use of a remote access Trojan called Gh0st RAT and linked it to previous attacks carried out in other countries, as well as prompting a prediction that further similar attacks would take place.

This last point exemplifies the value of a cyber kill chain; by analysing an attack in forensic detail it not only identifies the methods used and the history of such attacks but also provides a playbook for thwarting similar attacks in the future. The cyber-security experts at Littlefish will be able to execute a cyber kill chain in such a way as to identify how the impact of the attack could have been mitigated or the attack stopped in its tracks at each and every stage. When we work with an organisation to enhance their cyber security, we bring with us all the learning from cyber kill chains in the past and apply that learning to the security systems now in place. In a way it's simple – you get to benefit from what we've learned by studying other people's mistakes, and the *reactive* response of a cyber kill chain will enable your organisation to build a far more *proactive* response the next time your cyber security is threatened.