Task 1: Explain cyber kill chain stages.

Task 2: In which stage of the cyber kill chain is malware developed?

Task 3: Investigate the alternative frameworks.

A kill chain is a systematic process to target and engage an adversary to create desired effects. U.S. military targeting doctrine defines the steps of this process as find, fix, track, target, engage, assess (F2T2EA): find adversary targets suitable for engagement; fix their location; track and observe; target with suitable weapon or asset to create desired effects; engage adversary; assess effects (U.S. Department of Defense, 2007). This is an integrated, end-to-end process described as a “chain” because any one deficiency will interrupt the entire process.

Öldürme zinciri, bir düşmanı hedef almak ve etkilemek amacıyla kullanılan sistemli bir süreçtir. ABD askeri hedefleme doktrini, bu sürecin adımlarını bulma, sabitleme, izleme, hedefleme, angaje etme, değerlendirme (F2T2EA) olarak tanımlar: Hedeflenecek uygun düşman hedeflerini bul; konumlarını tespit et; izle ve gözle; istenen etkileri yaratmak için uygun silah veya araçla hedefle; düşmanı angaje et; etkileri değerlendir (ABD Savunma Bakanlığı, 2007). Bu, bir "zincir" olarak tanımlanan entegre, uçtan uca bir süreçtir, çünkü herhangi bir eksiklik tüm süreci kesintiye uğratacaktır.

Expanding on this concept, this paper presents a new kill chain model, one specifically for intrusions. The essence of an intrusion is that the aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives, be they moving laterally inside the environment or violating the confidentiality, integrity, or availability of a system in the environment. The intrusion kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives.

Bu konsepti genişleterek, bu makale özel olarak sızmalara yönelik yeni bir öldürme zinciri modeli sunmaktadır. Bir sızmanın özü, saldırganın güvenilen bir sınırı aşmak için bir yük geliştirmesi, güvenilen bir ortamın içinde bir varlık kurması ve bu varlık üzerinden amaçlarına yönelik eylemlerde bulunmasıdır, bu eylemler ortam içinde yan yana hareket etmek veya ortamdaki bir sistemin gizliliğini, bütünlüğünü veya erişilebilirliğini ihlal etmek olabilir. Sızma öldürme zinciri, keşif, silahlandırma, teslimat, sömürü, kurulum, komuta ve kontrol (C2) ve amaçlara yönelik eylemler olarak tanımlanır.

With respect to computer network attack (CNA) or computer network espionage (CNE), the definitions for these kill chain phases are as follows:

1. Reconnaissance - Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.

2. Weaponization - Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.

3. Delivery - Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors, as observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004-2010, are email attachments, websites, and USB removable media.

4. Exploitation - After the weapon is delivered to victim host, exploitation triggers intruders’ code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

Bilgisayar ağ saldırısı (CNA) veya bilgisayar ağ casusluğu (CNE) bağlamında, bu öldürme zinciri aşamalarının tanımları şu şekildedir:

1. **Keşif** - Hedefleri araştırma, tanımlama ve seçme, genellikle İnternet sitelerini taramayı içerir; bu siteler konferans bildirileri ve e-posta listeleri gibi kaynaklardan e-posta adresleri, sosyal ilişkiler veya belirli teknolojilerle ilgili bilgiler içerebilir.
2. **Silahlandırma** - Uzak erişim Truva atını bir saldırıyla birleştirerek teslim edilebilir bir yük oluşturma, genellikle otomatik araçlar (silahlandırıcı) aracılığıyla yapılır. Gittikçe artan bir şekilde, silahlandırılmış teslimat biçimleri olarak Adobe Taşınabilir Belge Biçimi (PDF) veya Microsoft Office belgeleri gibi istemci uygulama veri dosyaları kullanılır.
3. **Teslimat** - Silahın hedeflenen ortama iletilmesi. 2004-2010 yılları için Lockheed Martin Bilgisayar Olay Yanıt Ekibi (LM-CIRT) tarafından gözlemlenen APT aktörlerinin silahlandırılmış yükleri için üç en yaygın teslimat vektörü, e-posta ekleri, web siteleri ve USB taşınabilir ortamlardır.
4. **Sömürü** - Silah, kurban ana bilgisayarına teslim edildikten sonra, saldırganın kodunu tetikler. Genellikle, sömürü bir uygulama veya işletim sistem açığına yöneliktir, ancak aynı zamanda daha basitçe kullanıcıları sömürebilir veya kodu otomatik olarak yürüten bir işletim sistemi özelliğinden yararlanabilir.

5. Installation - Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.

6. Command and Control (C2) - Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have “hands on the keyboard” access inside the target environment.

7. Actions on Objectives - Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems

and move laterally inside the network.

1. **Kurulum** - Uzaktan erişim Truva atı veya arka kapı, düşmanın ortam içinde sürekliliği sağlamasına izin vermek amacıyla kurban sisteme kurulur.
2. **Komuta ve Kontrol (C2)** - Genellikle, tehlikeye düşen ana bilgisayarlar, bir C2 kanalı kurmak için dışa doğru sinyal göndermek zorundadır. APT kötü amaçlı yazılımları özellikle otomatik faaliyet yerine manuel etkileşim gerektirir. C2 kanalı kurulduktan sonra, saldırganlar hedef ortam içinde "klavye üzerinde elleri" olur.
3. **Amaçlara Yönelik Eylemler** - Ancak ilk altı aşamadan ilerledikten sonra, sızanlar orijinal amaçlarına ulaşmak için eylemlerde bulunabilirler. Tipik olarak, bu amaç veri dışa çıkarmayı içerir, bu da kurban ortamından bilgi toplamayı, şifrelemeyi ve çıkarmayı içerir; veri bütünlüğü veya erişilebilirliğinin ihlali de potansiyel amaçlardır. Alternatif olarak, sızanlar yalnızca ek sistemleri tehlikeye atmaya ve ağ içinde yan yana hareket etmeye yönelik bir atlama noktası olarak ilk kurban kutusuna erişim isteyebilir.