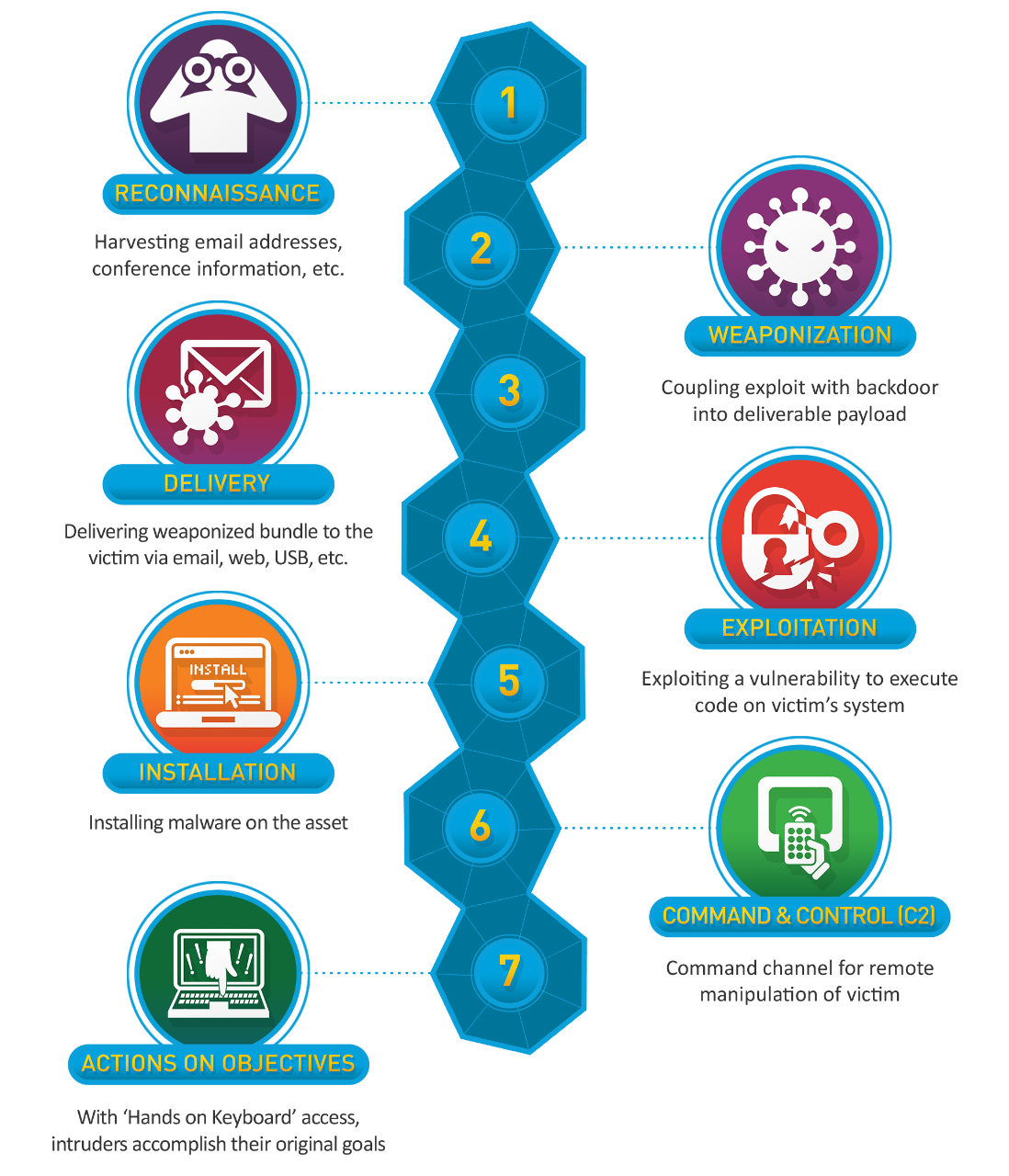
06.02.2025

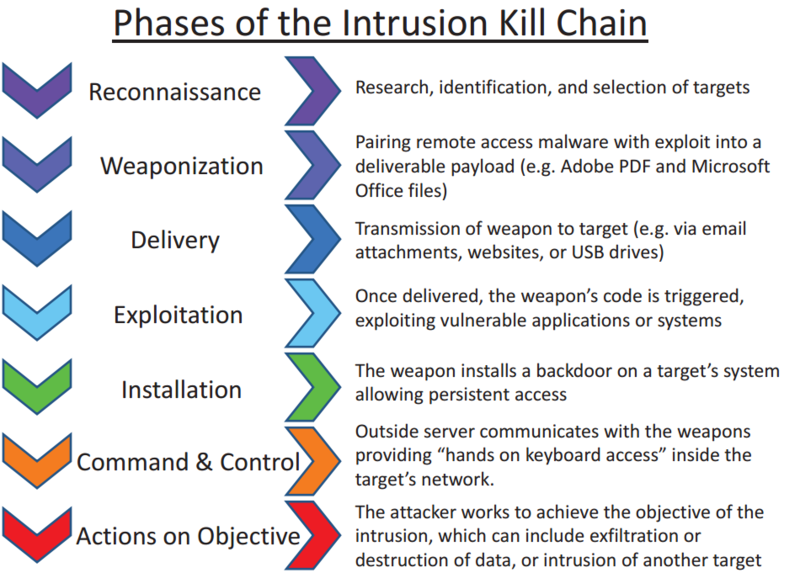


SOC Fundamentals & Cyber Kill Chain  
  
  
Şerif GÜL

Altay Takımı

**CYBER KİLL CHAİN**

**1. Giriş**

Siber güvenlikte etkin bir savunma stratejisi geliştirmek için siber saldırıların nasıl gerçekleştiğini anlamak kritik bir gerekliliktir. Lockheed Martin tarafından geliştirilen **Cyber Kill Chain** modeli, siber saldırıların yaşam döngüsünü ve bu sürecin her aşamasında savunma stratejileri oluşturmayı amaçlar.

**2. Cyber Kill Chain Aşamaları**

Cyber Kill Chain modeli yedi temel aşamadan oluşur. Her aşama, bir siber saldırının ilerlemesini ve savunma stratejilerini belirlemek için çok önemlidir.

**2.1. Reconnaissance (Keşif)**

* Saldırganlar, hedef sistem, ağ yapısı ve kullanıcılar hakkında bilgi toplar.
* OSINT (Open Source Intelligence) yöntemleri, phishing e-postaları ve sosyal mühendislik teknikleri kullanılabilir.
* **Savunma:** Tehdit istihbaratı, farkındalık eğitimleri ve veri sınırlandırma.

**2.2. Weaponization (Silahlandırma)**

* Saldırgan, hedefin zayıflıklarına uygun zararlı yazılımlar (örneğin, trojan veya exploit kitleri) geliştirir.
* **Savunma:** Güncellemelerin yapılması, zafiyet tespit sistemleri ve sandbox analizi.

**2.3. Delivery (Teslimat)**

* Zararlı içerik hedef sisteme iletilir (phishing, USB, drive-by-download vb.).
* **Savunma:** E-posta filtreleme, web güvenlik çözümleri, antivirüs yazılımları.

**2.4. Exploitation (Sömürme)**

* Saldırgan, hedef sistemde exploit kullanarak kod çalıştırır ve sistemi ele geçirir.
* **Savunma:** Zafiyet yönetimi, uygulama beyaz listeleme, EDR (Endpoint Detection and Response) sistemleri.

**2.5. Installation (Kurulum)**

* Saldırgan, kalıcılığı sağlamak için hedef sisteme backdoor veya RAT (Remote Access Trojan) gibi yazılımlar kurar.
* **Savunma:** Sistem izleme, davranış analizi, endpoint koruma mekanizmaları.

**2.6. Command & Control (C2C - Komuta ve Kontrol)**

* Saldırgan, sistemle uzaktan iletişim kurarak komutlar gönderir.
* **Savunma:** DNS trafiği analizi, anomali tespiti, IP kara listeleri.

**2.7. Actions on Objectives (Hedefe Ulaşma)**

* Saldırgan, veri çalıştırma, veri sızıntısı veya sistem bozulması gibi nihai amacını gerçekleştirir.
* **Savunma:** Veri kayıp önleme (DLP), ağ segmentasyonu, olay yönetimi.

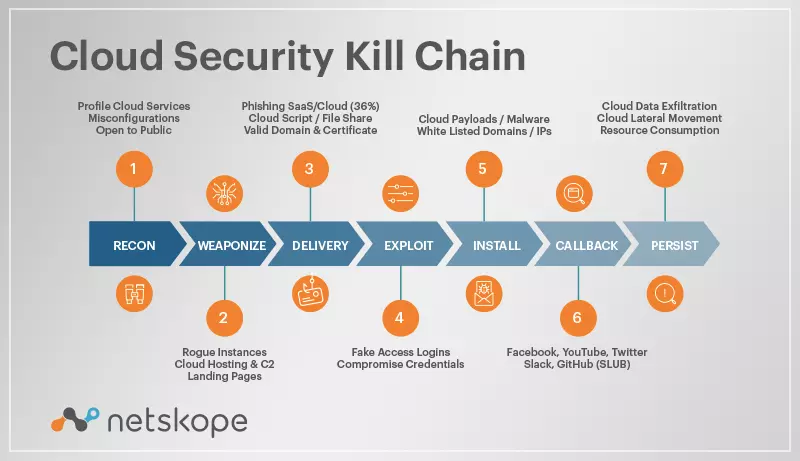
**3. SOC Analistleri için Cyber Kill Chain’in Önemi**

SOC analistleri için Cyber Kill Chain, olay tespiti ve müdahale süreçlerini optimize etmeye yardımcı olur:

1. **Erken Tespit:** Keşif ve teslimat aşamasında tespit edilen tehditler, sürecin ilerlemesini engelleyebilir.
2. **Katmanlı Savunma:** Her aşamada farklı savunma mekanizmaları uygulanabilir.
3. **Olay Yanıt Süreci:** Saldırının hangi aşamada olduğunu anlamak, müdahale stratejilerini belirler.

**4. Gerçek Dünya Senaryosu ve Proaktif Savunma**

* **SOC Senaryosu: Çok Aşamalı Siber Saldırı Müdahalesi**
* **Olay Kodu: INC-2023-067** **Tarih: 20 Kasım 2023  
  Zaman Dilimi: 09:00 - 14:00**
* **1. Teslimat Aşaması: E-posta Filtreleme Sistemlerinin Yetersiz Kalması**
* **Olay Tespiti**
* **09:15: E-posta güvenlik ağ geçidinden (Proofpoint) gelen uyarı:**
* **user2@firma.com adresine şüpheli bir e-posta ulaştı ("Önemli: Staj Başvuru Sonuçları Ektedir").**
* **Ek: Staj\_Sonucu.pdf.exe (SHA-256: d4e5f6...).**
* **Filtreleme hatası: E-posta, "PDF" uzantılı gibi görünen ancak EXE içeren bir dosya nedeniyle atlatıldı.**
* **Analiz ve Müdahale**
* **SOC Analisti (L1):**
* **E-posta başlığını inceledi: Gönderen IP (94.156.33.22) geçersiz SPF kaydına sahip.**
* **Dosyayı sandbox ortamında çalıştırdı: Dosya, kullanıcı verilerini C2 sunucusu: 167.86.99.12’ye sızdırmaya çalıştı.**
* **Acil Adımlar:**
* **Tüm kullanıcılara "Bu e-postayı açmayın!" uyarısı gönderildi.**
* **E-posta, tüm posta kutularından otomatik silindi (Microsoft 365 Güvenlik Merkezi).**
* **2. Sömürme Aşaması: Zafiyetin Aktif Kullanımı**
* **Olay Tespiti**
* **10:30: IDS/IPS sisteminden gelen uyarı:**
* **192.168.33.15 IP’li cihazda CVE-2023-1234 (Microsoft Office zafiyeti) sömürülmeye çalışıldı.**
* **Hedef: \\fileserver\HR dizinine yetkisiz erişim denemesi.**
* **Analiz ve Müdahale**
* **SOC Analisti (L2):**
* **Saldırının kaynağı: 94.156.33.22 (e-posta göndereni ile aynı IP).**
* **Sistemdeki Office yazılımının güncel olmadığı tespit edildi (Nessus Tarama Raporu).**
* **Acil Adımlar:**
* **Zafiyetli yazılımlar güncellendi.** 
* **192.168.33.15 izole edildi ve bellek dump’ı alındı (FTK Imager).**
* **3. Kurulum Aşaması: Zararlı Yazılım ve C2 İletişimi**
* **Olay Tespiti**
* **11:45: EDR (CrowdStrike) uyarısı:**
* **192.168.33.15 üzerinde svchost.exe prosesi anormal ağ bağlantıları oluşturuyor.**
* **DNS sorgularında malicious-domain[.]xyz tespit edildi.**
* **Analiz ve Müdahale**
* **SOC Analisti (L3):**
* **Zararlı yazılım: Remcos RAT (Uzak Erişim Truva Atı).**
* **C2 iletişimi: TCP/8080 üzerinden XOR şifreli trafik.**
* **Acil Adımlar:**
* **Güvenlik duvarından malicious-domain[.]xyz ve 167.86.99.12 engellendi.**
* **Zararlı proses sonlandırıldı ve kayıt defteri temizlendi.**
* **Tüm ağda IOC (Indicator of Compromise) taraması yapıldı (Velociraptor).**
* **4. Genel Müdahale ve İyileştirme**
* **13:00:**
* **Olay Raporu: Saldırı, "phishing → exploit → C2" zinciriyle gerçekleşti.**
* **Öneriler:**
* **E-posta filtreleme sistemlerine Yapay Zeka tabanlı sandbox entegrasyonu.**
* **Tüm cihazlarda otomatik güncelleme politikası zorunlu hale getirilecek.**
* **Kullanıcılara phishing simülasyon eğitimi verilecek.**



**Kaynakça:**

codark.netlockheedmartin.com

Gaissecurity.com

springboard.com

Wikipedia.com

Netskope.com

chatgpt.com