Türk Telekom Siber Güvenlik Kampı
Siber tehdit İstihbaratı Ödev

1) a. MD5: cb84fc4682a74ba81ef477bc1359959b
   Fox Kitten
   https://analyze.intezer.com/analyses/af4602e7-7e86-41cc-980a-417b30f8351b
   https://otx.alienvault.com/indicator/file/cb84fc4682a74ba81ef477bc1359959b
   https://attack.mitre.org/groups/G0117/
   https://www.virustotal.com/gui/file/40ba95b54dc4cf0754efcfaeef3bbd71aac65882f3c92b8814a82ea02969da84/details
   https://malshare.com/sample.php?action=detail&hash=cb84fc4682a74ba81ef477bc1359959b

   b. MD5: 836d61745e087e6017832233701218a4
   Fox Kitten
   https://analyze.intezer.com/analyses/d594dbb0-11ec-4872-9578-aa0e9536f6a3
   https://otx.alienvault.com/indicator/file/836d61745e087e6017832233701218a4
   https://attack.mitre.org/groups/G0117/
   https://www.virustotal.com/gui/file/0a12cd6b5c85dbf65e524507429163e35818943aea6e81aa5a9c5205391d256c/community
   https://malshare.com/sample.php?action=detail&hash=836d61745e087e6017832233701218a4

2) T1190 - Exploit Public-Facing Application, T1078 - Valid Accounts
   https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0117%2FG0117-enterprise-layer.json

3) Tehdit istihbaratı, saldırganlarını daha iyi anlamak, olaylara daha hızlı yanıt vermek ve bir tehdit aktörünün bir sonraki hamlesinin proaktif olarak önüne geçmek için tehdit verilerinin işlenmesine yardımcı olarak her şekil ve büyüklükteki kuruluşa fayda sağlar. KOBİ'ler için bu veriler, aksi takdirde ulaşamayacakları bir koruma düzeyine ulaşmalarına yardımcı olur. Öte yandan, büyük güvenlik ekiplerine sahip kuruluşlar, dış tehdit istihbaratından yararlanarak maliyeti ve gerekli becerileri azaltabilir ve analistlerini daha etkili hale getirebilir.

4) Askeri, ticari veya güvenlik bağlamında istihbarat, bir kuruluşa karar desteği ve stratejik bir avantaj sağlayan bilgilerdir. Tehdit istihbaratı, daha büyük bir güvenlik istihbaratı stratejisinin bir parçasıdır. Bir kuruluşu dış ve iç tehditlerden korumaya ilişkin bilgilerin yanı sıra bu bilgileri toplamak ve analiz etmek için kullanılan süreçleri, politikaları ve araçları içerir.
   Tehdit istihbaratı, güncel taktikleri, teknikleri ve prosedürleriyle birlikte tehdit ortamı ve tehdit aktörleri hakkında daha iyi bilgi sağlar. Gelişmiş saldırıları ve sıfırıncı gün tehditlerini tespit etmek ve önlemek için kuruluşların güvenlik kontrollerini yapılandırmada proaktif olmalarını sağlar. Bu uygulamaların çoğu otomatikleştirilebilir, böylece güvenlik gerçek zamanlı olarak en son istihbaratla uyumlu kalır.

Faruk Ulutaş