Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Açık Kaynak İstihbaratı Üzerinden Siber Saldırı Tespiti Yöntemleri

Ali EKŞİM [a,b*], Mustafa KARA [b,c]

[a] *TÜBİTAK BİLGEM UEKAE, PK 74, 41470 Gebze, Kocaeli, TÜRKİYE*
[b] *MSÜ, Hezârfen Havacılık ve Uzay Teknolojileri Enstitüsü, İstanbul, TÜRKİYE*
[c] *Mustafa Kemal Üniversitesi, Hatay, TÜRKİYE*
** Sorumlu yazarın e-posta adresi: ali.eksim@tubitak.gov.tr*

ÖZET

Son yıllarda siber suçun gittikçe büyüyen etkisi, siber tehditlerin üstesinden gelmek için dünya çapında istihbarat ve kanun uygulayıcı kurumlar ortaya çıkartmıştır. Tüm kurum ve kuruluşlar siber suçla en iyi şekilde nasıl mücadele edileceğini öğrenmeye çalışmaktadır. İnternet ağ teknolojilerinin gelişmesi ve genişlemesi ile siber saldırıları engellemek gittikçe zorlaşmaktadır. Ağdaki tehlikeli hedeflerin kapsamlı bir analizini oluşturmak için internette açık halde bulunan verileri toplayarak istihbarat elde etmek, istihbarat birimleri için önemli bir araç olarak hızla gelişmektedir. İnternetteki mevcut açık kaynakların miktarı hızla arttıkça, siber suçla mücadele gelişen açık kaynak istihbaratı yani OSINT yöntemleri çerçevesinde daha etkin olmaktadır. Buna bağlı olarak bilginin etkili ve verimli bir şekilde toplanması ve işlenmesi için gelişmiş yazılım araçları ve teknikleri daha da gelişmektedir. Bu çalışmada, OSINT kavramı siber saldırı tespiti için her açıdan ele alınmıştır. OSINT kavramını internet ortamında kamuya açık paylaşılan veriler üzerinden tarama, bulma, toplama, çıkarma, kullanma, doğrulama ve analiz yaparak elde etme amaçlı destek yöntemleri detaylandırılarak anlatılmıştır. Siber tehditlere karşı geliştiren araştırmalar için açık kaynak verilerinin kullanılmasına yönelik mevcut çabalar gözden geçirilmiş ve detaylı bir şekilde incelenmiştir. Bunlara ek olarak, siber suçlarla etkin mücadele için siber suç soruşturma çerçevesi önerilmiştir.

Anahtar Kelimeler: *Açık Kaynak İstihbaratı, Güvenlik, OSINT, Saldırı Tespiti, Siber Savunma*

Cyber Attack Detection Methods over Open Source Intelligence

ABSTRACT

In recent years, the growing impact of cybercrime has revealed worldwide intelligence and law enforcement agencies to overcome cyber threats. All institutions and organizations are trying to learn how to fight cybercrime in the best possible way. With the development and expansion of internet networking technologies, it becomes increasingly difficult to prevent cyber attacks. It is rapidly developing as an important tool for intelligence units by collecting data on the internet to generate a comprehensive analysis of dangerous targets on the network. As the amount of available open-source resources on the internet increases rapidly, the emerging open-source intelligence, in other words, is more effective within the framework of OSINT methods. In this connection,

Geliş:10/12/2018, Düzeltme:13/01/2019, Kabul: 17/01/2019

advanced software tools and techniques are further developed for the effective and efficient collection and processing of information. In this study, the concept of OSINT was discussed in all aspects for cyber attack detection. The purpose of browsing, finding, collecting, extracting, using, verifying and analyzing the OSINT concept through publicly available data is explained in detail. Existing efforts to use open source data for research against cyber threats have been reviewed and examined in detail. In addition, the cyber crime investigation framework has been proposed to combat cybercrime effectively.

Keywords: *Open Source Intelligence, Security, OSINT, Attack Detection, Cyber Defense*