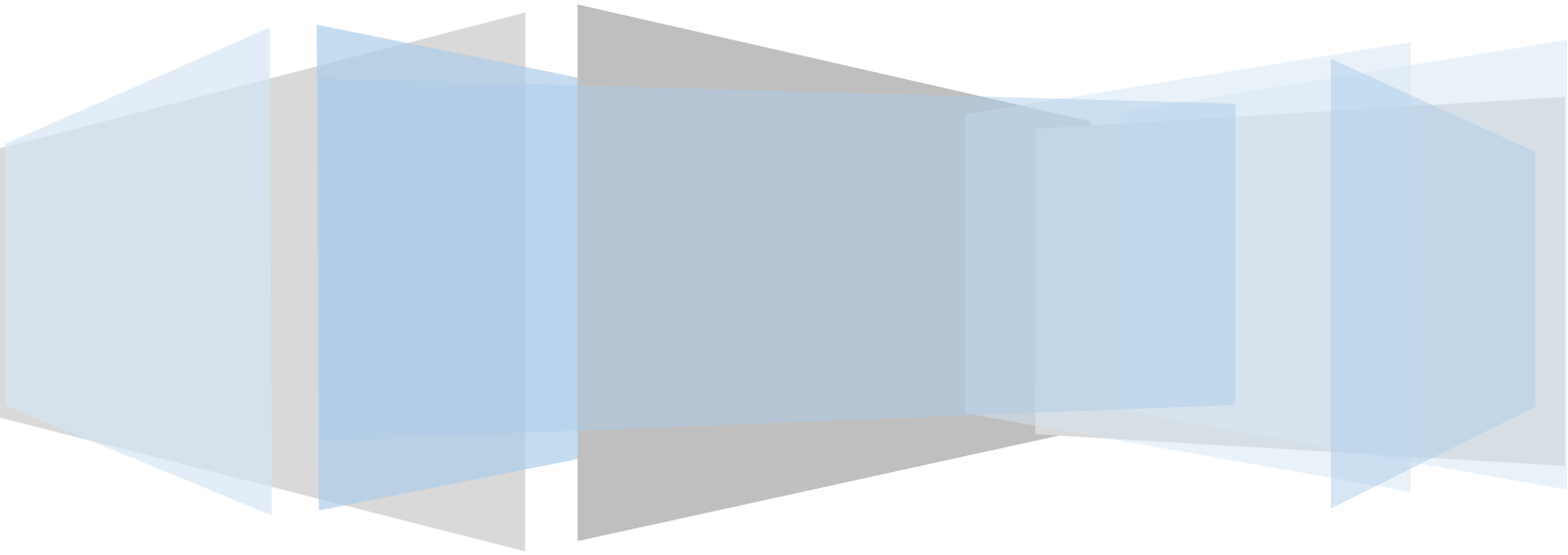
NETAS | Bilişim Teknolojileri

Siber Güvenlik Hizmetleri Direktörlüğü

Lyceum Hexane Vaka Analiz Önizlemesi

Sürüm 1.0

28/08/2019



Gizli Başlangıç Tarihi: Mayıs 2019
Bitiş Tarihi: Devam Ediyor
Güvenlik Vakası: Lyceum&Hexane Grubu Ortadoğu Bölgesi Odaklı Atakları
Vaka Tipi: ATP

Netaş Bilişim Teknolojileri A.Ş.
Orhanlı Mah. İrfan Cad. No: 28
Tuzla / İstanbul
T: +90 216 522 58 74
F: +90 216 329 08 14
E: info@netasbilisim.com.tr
www.netasbilisim.com.tr

VAKA ÖNİZLEMESİ

Öncelikli olarak kritik altyapı sistemlerini -ICS (Industrial Control Systems) ve OT (Operational Technology)- hedef aldığı bilinen ve ilk adı Hexane olarak yayınlanmış Lyceum tehdit aktörü, 2019 yılı Mayıs ayı içerisinde Ortadoğu bölgesinde yer alan kurumları hedef alan ilk aktiviteleriyle tespit edilmiştir. Lyceum grubunun aktiviteleri, daha öncesinde siber tehdit ve etki analizi raporları sizlerle paylaşılmış APT34-Oilrig grubuyla bağdaştırılsa da, tespit edilen aktiviteler çok yeni ve az veriye sahip olduğu için kesin bir atama yapılamamıştır. Grubun 2018 yılından beri aktif olduğu ve bu yıl içerisinde Güney Afrika hedefli saldırılar gerçekleştirdiği bilinmektedir. Teknik, taktik ve prosedürlerinde keskin geliştirmeler görülen grubun Ortadoğu bölgesindeki aktivitelerine dair ilk bulgular ise, 2019 Ağustos ayı itibariyle paylaşılmaya başlanmıştır.

Lyceum grubu tarafından kullanılan enfeksiyon taktikleri, oltalama kampanyaları ve password spraying olarak belirlenmiştir. Password spraying bir parola tahmini atağıdır ve kullanıcının bir parolayı birden fazla platformda kullanması zayıflığından yararlanmaktadır. Herhangi bir platformda yaşanan veri sızıntısı ardından elde edilen kullanıcı parolası, aynı e-posta adresiyle kullanıcı hesabı olma ihtimali bulunan diğer platformlarda ve çalıştığı kurum hesabında da denenerek giriş yapılmaya çalışılır. Lyceum grubu tarafından gerçekleştirilen oltalama saldırıları ise, özellikle İnsan Kaynakları ve Bilgi Teknolojileri departmanlarını hedef alan, doğrudan bu departmanları ilgilendiren içerikler ile hazırlanmış ve zararlı kod içeren dökümanlar aracılığıyla gerçekleştirilmektedir.

Grup tarafından başarıyla enfekte edilen kullanıcı cihazları üzerinde, saldırganlar tarafından her türlü işlem gerçekleştirilebilmektedir. Hedef alınan İnsan Kaynakları departmanında yer alan bir kullanıcı hesabının enfekte edilmesi ve parolasının elde edilmesi sonucunda, kurum içerisinde yer alan hassas verilere ulaşılması mümkün olmaktadır. Hedef alınan bir diğer departman olan Bilgi Teknolojileri kullanıcıları hesaplarının enfekte edilmesi durumunda ise, kuruma ait diğer sistemlere sızılması ya da yetkili kullanıcı hesaplarının ele geçirilmesi durumları mümkün olmaktadır.

Netaş Bilişim Teknolojileri A.Ş.
Orhanlı Mah. İrfan Cad. No: 28
Tuzla / İstanbul
T: +90 216 522 58 74
F: +90 216 329 08 14
E: info@netasbilisim.com.tr
www.netasbilisim.com.tr