Kaspersky APT İstihbarat Raporlaması

kaspersky GELECEĞİ YAKALAYIN

Kaspersky APT İstihbarat Raporlaması

Kaspersky APT İstihbarat Raporlaması müşterileri, keşfedilen her APT ile ve kesinlikle kamuya açıklanmayacak tehditlerle ilgili tüm teknik veriler (çeşitli biçimlerde) dahil olmak üzere incelemelerimize ve keşiflerimize benzersiz bir sürekli erişim olanağına sahip olur. Raporlar, güvenlik araştırmacılarına, kötü amaçlı yazılım analistlerine, güvenlik mühendislerine, ağ güvenliği analistlerine ve APT araştırmacılarına tehditlere karşı hızlı ve doğru müdahale edilmesini sağlayan eyleme geçirilebilir veriler sunmak için ilgili APT ile birlikte APT'nin ilgili IOC'leri ve YARA kurallarını içeren ayrıntılı bir teknik açıklamasını sunan C düzeyi odaklı ve anlaşılması kolay bilgiler veren bir yönetici özeti içerir.

Uzmanlarımız siber suçlu gruplarının taktiklerinde tespit ettikleri herhangi bir değişiklik konusunda da sizi anında uyaracaktır. Güvenlik savunmanızın başka bir güçlü araştırma ve analiz bileşeni olan, Kaspersky'nin eksiksiz APT raporları veri tabanına da erişiminiz olacaktır.

Avantajlar

MITRE ATT&CK
Raporlarda açıklanan tüm TTP'ler, MITRE ATT&CK ile eşlenerek ilgili güvenlik izleme kullanım durumlarının geliştirilmesi ve önceliklendirilmesi, açık analizlerinin yapılması ve mevcut savunmaların ilgili TTP'lere karşı test edilmesi yoluyla daha iyi algılama ve müdahale sağlar

Genel kullanıma açık olmayan APT'ler hakkında bilgi
Çeşitli nedenlerle, yüksek profilli tehditlerin tamamı hakkında kamuya bilgi verilmez. Fakat bunları müşterilerimizle paylaşırız

Ayrıcalıklı erişim
Kamuya açıklanmadan önce, devam eden araştırmalar sırasında tespit edilen en son tehditler hakkında teknik açıklamalar alın

Geriye dönük analiz
Abonelik döneminiz boyunca, önceden hazırlanan tüm özel raporlara erişim olanağı sunulur

Teknik verilere erişim
OpenIOC veya STIX'i de içeren standart biçimlerde sunulan genişletilmiş bir IOC listesine ve YARA kurallarımıza erişim dahildir

Tehdit aktörü profilleri
Şüpheli kaynak ülke ve ana faaliyet, kullanılan kötü amaçlı yazılım aileleri, hedeflenen sektörler ve coğrafyalar ve MITRE ATT&CK ile eşleme ile birlikte, kullanılan tüm TTP'lerin açıklamaları dahildir

Sürekli APT kampanya izleme
Araştırma sırasında eyleme dönüştürülebilir istihbarata erişim (APT dağıtımı, IOC'ler, komut ve kontrol altyapıları vb. hakkında bilgi).

RESTful API
Güvenlik iş akışlarınızın sorunsuz entegrasyonu ve otomasyonu

www.kaspersky.com.tr