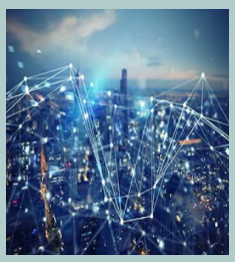
Kale İleri Teknoloji Siber Güvenlik Bülteni

KALE İLERİ TEKNOLOJİ

Cilt 1,Sayı 2

Bülten Tarihi: 31.12.2021

Sektörden Haberler



⇒ Gelişmiş bir zararlı yazılım olan NginRAT , Nginx sürecinde gizlenerek çalıştığı tespit edilmiştir.

⇒ Çin merkezli bir APT grubunun 42 adet alan adını saldırılarda kullandığı tespit edilmiştir. Grup APT15, Bronze Palace, Ke3Chang, Mirage, Payful Dragon ve Vixen Panda olarak da isimlendirilmektedir.

⇒ Wordpresste 4 tane plugin ve 15 Epsilon Framework temasındaki zafiyetlerden yararlanılarak 1,6 milyona kadar WordPress sitesi siber saldırılarda hedef alındı.

⇒ Kötü niyetli aktörler Microsoft Exchange Outlook Web Access sunucusunda kullanıcı adı ve parola çiftlerini çalmak, uzaktan komut çalıştırmayı aktifleştirmek için IIS Web sunucusunun bir modülü olan Owowa'yı kullanıyorlar.

⇒ Azure Uygulama Hizmetinde 2017 Eylülden bu yana devam eden bilgi sızıntısı zafiyeti tespit edildi.

İlgi çeken özel konular:

- Sektörden Haberler
- Etkinlik
- Siber Tehdit İstihbaratı
- Siber Güvenlik Yazıları

Bu sayıda:

Yeni Çıkan Zafiyetler

⇒ Araştırmacılar tarafından Apple, Safari, Firefox, Tor Browser vb. tarayıcılarının etkilendiği 14 yeni siteler arası veri sızıntısı zafiyeti keşfedildi.

⇒ Araştırmacılar tarafından log4j zafiyeti (CVE-2021-44228) bulundu. Bu zafiyetle uzaktan komut çalıştırılabilmektedir.

⇒ Windows Active Directory Domain servisinde yetki yükseltmek için CVE-2021-42287 ve CVE-2021-42278 zafiyetleri bulundu.

⇒ Garrett Metal Dedektörlerinde yapılandırmada değişiklik yapılmasını ve uzaktan komut çalıştırılmasını sağlayan zafiyetler bulundu.

⇒ İkinci log4j zafiyeti (CVE-2021-45046) bulundu. Bu zafiyetle diğer log4j zafiyetinde olduğu gibi uzaktan komut çalıştırılabilmektedir.

Siber Tehdit İstihbaratı

En sık kullanılan C&C Sunucularının IP adresleri:

144.91.122.102
103.208.86.148
80.211.3.13
103.208.86.151
79.173.195.234
45.15.23.184
139.59.14.223
37.210.226.125
54.37.212.235
187.162.59.232
162.214.50.39
103.139.242.30
120.50.40.185

Siber Güvenlik Blog Yazıları

Aralık ayında Medium Blog sayfamızda yayınladığımız yazılar:

Sysmon — Sysmon Kurulumu

Sysmon — Sysmon Events

Sysmon — Reverse Shell Analizi

Sysmon — MS17–010 Exploit Analizi

Sysmon — Kullanıcı İşlemleri Analizi

Sysmon — Detaylı Komut Analizi

Sysmon — Exploit Edilmiş Bir Sistemde Servis ile Kalıcılık ve Analizi

Sysmon — Exploit Edilmiş Bir Sistemde Registry ile Kalıcılık ve Analizi

Sysmon — Exploit Edilmiş Bir Sistemde Volume Shadow Copy Aracılığıyla Kalıcılık ve Log Analizi

Sysmon — RID Hijacking İşlemi ve Analizi

Sysmon — Sysmon Tools

Python Uygulama

Anomali Staxx üzerinden IOC bilgilerini çekmek için aşağıdaki python kodunu kullanabilirsiniz:

```
import requests
import json
url="https://<IP_adresi>:8080/login_request"
data={"username":"admin","password":"changeme"}
header={"Content-Type": "application/json"}
sonuc=requests.post
(url=url,headers=header,data=json.dumps
(data),verify=False)
cookie =  sonuc.headers['Set-Cookie']
cookies= cookie.split(";")[0]
url="https://10.10.10.40:8080/search/result/"
header={"Content-Type":                    "application/
json","Cookie":cookies}
data={"searchstr":"","severity":["very-
high"],"confidence":50,"interval":"7d","tlp":[],"source":
[],"itype":[]}
sonuc=requests.post
(url=url,headers=header,data=json.dumps
(data),verify=False)
for ioc in  sonuc.json()['data']:
     print ioc['indicator']
     print ioc['severity']
     print ioc['feed_name']
```

KALE İLERİ TEKNOLOJİ

Kızılırmak Mahallesi Ufuk Üniversitesi Caddesi No:8/4 Çukurambar Çankaya/ Ankara

Telefon: 0 (312) 287 97 18
Faks: 0 (312) 287 97 19
E-posta: info@kaleileriteknoloji.com.tr

Siber Güvenlikte Yerli ve Milli Çözüm

KALE İLERİ TEKNOLOJİ

2016 yılında kurulan Kale İleri Teknoloji, sürekli gelişmekte olan teknoloji ile birlikte kurumsal verileri güvenli bir şekilde işlemek, saklamak, iletmek ve bu alanda sürekli yenilenen tehditlere karşı aksiyon almak, günlük operasyonların yürütülebilmesi için elektronik ortama taşınan ve işlenen verinin gizliliği, erişimlerinin doğru bir şekilde yetkilendirilmesi, bütünlüklerinin sağlanması amacıyla, müşterilerinin talepleri doğrultusunda uzman kadrosu ve en son teknoloji imkanlarıyla birlikte hedef odaklı çözümler geliştirme, yenilikçi bakış açısıyla amaca yönelik siber güvenlik eğitimleri verme, siber güvenlik alanında ihtiyaç duyulan uygulamalar geliştirme ve müşterilerinin güvenliğini optimize etmek için danışmanlık hizmetleri sunma yolundaki çalışmalarını sürdürmektedir.

Neden Kale İleri Teknoloji?

Vizyonumuz:

Siber ağlar, bireysel ve toplumsal, özel ve kamusal, yerel ve global her türden ve her dereceden tüm varlıkların nöral hafıza, bilinç, zeka ve ileti ağlarıdır. Siber çağda tüm kurumların varlığı siber ağlardaki evrimi ve güvenliğine bağlıdır. Siber güvenlik, siber çağda her tür bireysel ve kurumsal varlığın yaşam güvenliğidir. Kale İleri Teknoloji, siber teknolojilerin fizyolojik, biyolojik, psikolojik, sosyal ve siyasal dünyayı yeni baştan nasıl inşa ettiğinin bilinciyle öngörülerini, beklentilerini ve hayallerini rasyonalitesine yükleyen bir firmadır.

Misyonumuz:

Kale İleri Teknoloji, siber teknik altyapısı ve uzman kaynağıyla, evrensel insanlık değerlerine saygılı, siber çağın gereklerine uygun, siber tehdit analizleri, siber tehdit öngörüleri ve siber çözüm ve ürün Ar-Gesiyle teknolojik dönüşüme katkı sağlayan ve müşterilerinin bilişim güvenliğinde yüksek performans gösteren, alanında global lider bir firma olmayı misyon edinmiş bir firmadır.