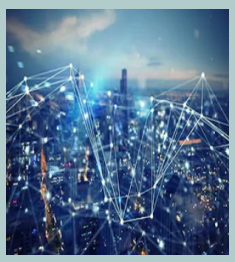
Kale İleri Teknoloji Siber Güvenlik Bülteni

KALE İLERİ TEKNOLOJİ

Cilt 1, Sayı 1

Bülten Tarihi: 30.11.2021

Sektörden Haberler



⇒ 9 milyondan fazla Android cihaza , cihaz bilgilerini , cep telefonu bilgilerini ele geçirmek için Huawei'nin AppGallery pazarında oyun teması altında çok sayıda zararlı yazılım tespit edildi.

⇒ GoDaddy firmasında 2018 yılından bu yana meydana gelen üçüncü güvenlik olayı, 1.2 milyon aktif ve aktif olmayan müşterinin verilerine yetkisiz erişimle sonuçlanan bir veri ihlali , meydana geldi.

⇒ Tehdit aktörleri, spam kampanyalarında kullanabilmek için Microsoft Exchange Sunucularını etkileyen ProxyShell (CVE-2021-34523) ve ProxyLogon(CVE-2021-26855) zafiyetlerinden yararlanmaktadırlar.

Yeni Çıkan Zafiyetler

⇒ Abdelhamid Naceri tarafından tespit edilen CVE-2021-41379 koduna sahip zafiyet ile herhangi bir yürütülebilir dosyayı bir MSI yükleyici dosyasıyla değiştirerek, bir saldırganın SYSTEM ayrıcalıklarıyla kod çalıştırılabilmektedir.

⇒ vSphere Web Client tarafında CVE-2021-21980 kodu ile tanımlanan zafiyet bulundu, vCenter Server 6.5 ve 6.7 versiyonları etkilenmektedir.

⇒ 11 tane zararlı Python Kütüphanesi tespit edildi. Bu Python kütüphaneleri:

- Importantpackage
- important-package
- pptest
- ipboards
- owlmoon
- DiscordSafety
- trrfab
- 10Cent10
- 10Cent11
- yandex-yt
- yiffparty

İlgi çeken özel konular:

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

Bu sayıda:

Yeni Çıkan Zafiyetler

⇒ Palo Alto Networks GlobalProtect VPN'de yetkisiz bir şekilde komut çalıştırmaya izin veren bir zafiyet bulundu. CVE-2021-3064 kodu ile incelenebilen zafiyet PAN-OS 8.1.17'den önceki PAN-OS 8.1 sürümlerini etkiler.

⇒ Microsoft Exchange Server üzerinde uzaktan komut çalıştırmaya izin veren CVE-2021-42321 koda sahip zafiyet bulundu.

⇒ Linux Kernel TIPC(Transparent Inter Process Communication) modülü üzerinde uzaktan komut çalıştırmaya izin veren bir zafiyet bulundu. CVE-2021-43267 kodu ile incelenebilir.

⇒ Gitlab üzerinde CVE-2021-22205 koduna sahip uzaktan komut çalıştırma zafiyeti bulundu. 11.9 sürümünden itibaren Gitlab bütün sürümleri etkilenmek olup; 13.8.8, 13.9.6 ve 13.10.3 sürüm numaralarında zafiyet giderilmiştir.

Etkinlik

22–26 Kasım 2021 tarihleri arasında düzenlenen Siber Güvenlik Haftası kapsamında Kale İleri Teknoloji olarak Siber Güvenlik İçin Python ve Tehdit Avcılığına Giriş eğitimlerini YouTube üzerinden verilmiştir.

Siber Güvenlik İçin Python Eğitimini aşağıdaki linkten izleyebilirsiniz:
https://www.youtube.com/watch?v=bvj-PvDkd3s

Siber Güvenlik İçin Python Eğitiminde yazdığımız kodlara aşağıdaki link üzerinden erişebilirsiniz.
https://github.com/kaleakademi/siber-guvenlik-icin-python-egitimi

Tehdit Avcılığına Giriş eğitimimizi aşağıdaki link üzerinden izleyebilirsiniz.
https://www.youtube.com/watch?v=YRImwydbCFk

Siber Tehdit İstihbaratı

En sık kullanılan C&C Sunucularının IP adresleri:

103.77.205.102
110.172.137.20
129.208.184.37
14.102.188.227
146.66.139.84
162.33.177.123
162.33.177.152
162.33.177.158
162.33.177.178
162.33.178.119
162.33.178.131
162.33.178.137
162.33.178.179
162.33.178.246
162.33.179.12
162.33.179.2
162.33.179.210
162.33.179.237
162.33.179.253
164.90.174.188
164.90.229.209
181.118.183.60
181.176.174.139
191.36.151.129
194.36.28.26
200.127.27.220
202.179.185.203
212.175.98.171
31.220.49.39
49.156.39.150
51.91.142.158
67.207.95.35
73.171.4.177

Siber Güvenlik Blog Yazıları

Kasım ayında Medium Blog sayfamızda yayınladığımız yazılar:

Windows Log Analizi — Reverse Shell Analizi

Windows Log Analizi — MS17–010 Exploit Analizi

Windows Log Analizi — Kullanıcı İşlemleri Analizi

Windows Log Analizi — Exploit Edilmiş Bir Sistemde Servis ile Kalıcılık ve Analizi

Windows Log Analizi — Exploit Edilmiş Bir Sistemde Registry ile Kalıcılık ve Analizi

Windows Log Analizi — Exploit Edilmiş Bir Sistemde Task Scheduler ile Kalıcılık ve Analizi

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

Windows Log Analizi — Exploit Edilmiş Bir Sistemde Startup File ile Kalıcılık ve Analizi

Windows Log Analizi — Detaylı Komut Analizi

Windows Log Analizi —APT -Hunter

Windows Log Analizi — Audit Policy Değişikliği Tespiti

Windows Log Analizi — OpenSSH Server Kurulumu ve Putty Bağlantı Analizi

Windows Log Analizi — RID Hijacking İşlemi ve Analizi

Python Uygulama

Versiyon taraması ve taramada yeni bulunan IP adreslerini bir dosyaya kaydeden python kodu aşağıdaki şekildedir:

```
# -*- coding: utf-8 -*-
import socket
banner_liste=[]
IP=raw_input("Ip adresini giriniz:")
baslangic_port=input("Baslangic port:")
bitis_port=input("Bitis port:")
for port in range(baslangic_port,bitis_port):
   try:
          soket = socket.socket()
          soket.connect((IP,port))
          banner=str(soket.recv(1024))
          print "[+]Port:",str(port)
          print "[+]Banner:",banner
          banner_liste.append(str(banner))
          print "Yeni IP adresi kontrolü"
          dosya = open("yeni_ip.txt","r")
          icerik = dosya.read()
          dosya.close()
          if not str(IP) in icerik:
                 dosya = open("yeni_ip.txt","a")
                 veri = IP+"\n"
                 dosya.write(veri)
                 dosya.close()
          soket.close()
   except:
          pass
```

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.