SOCRadar®

2021

SOCRadar Tehdit Yüzeyi Raporu

TÜRKİYE

İÇİNDEKİLER

Özet

Asya ve Avrupa arasında stratejik bir konuma sahip olan Türkiye, birbirine bağlı bir dünyada APT grupları tarafından gerçekleştirilen sofistike siber saldırılara karşı bağışık olmaktan uzak. Ülkedeki genç nüfusun hızla dijitalleşmesi, potansiyel saldırı yüzeylerini her geçen gün daha da artırıyor.

SOCRadar'ın hazırladığı bölgesel siber tehdit raporları, birden fazla bölgede faaliyet gösteren kuruluşlardaki güvenlik uzmanlarının karar verme mekanizmalarını iyileştirmek için bölgelerindeki tehdit ortamını daha iyi anlamalarını sağlıyor. Bu rapordaki bilgiler, kurumsal çapta güvenlik programlarının planlanmasına, yatırım kararları alınmasına ve siber güvenlik gereksinimlerinin tanımlanmasına yardımcı oluyor.

SOCRadar söz konusu tehdit ortamını, açık tehdit paylaşım platformlarından topladığı ve kapsamlı veri izleme, toplama, sınıflandırma ve analiz yöntemleriyle derlediği bilgiler doğrultusunda "yakın zamanda gözlemlenen tehdit aktörü faaliyetleri, kötü amaçlı yazılım kampanyaları, yeni kritik güvenlik açıkları, açıklardan yararlanma" temelinde inceliyor.

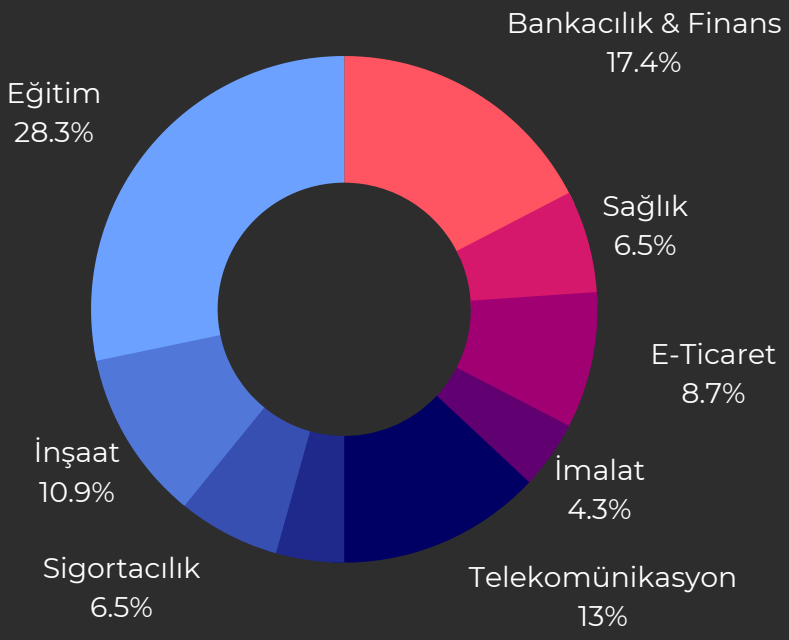
SOCRadar CTIA Ekibi, rakiplerini ve TTP'lerini anlama konusundaki benzersiz bakış açısı sayesinde dark/deep web tehdidi araştırması, HUMINT gözlemleri, siber güvenlik satıcısı blogları ve sosyal medya trendleri hakkında topladığı bilgileri bu raporda bir araya getiriyor.

Önemli Bulgular

- Türk varlıklarını hedef alan 30 tehdit aktörünün 150'den fazla listesi var. Gönderilerin %22'si müşteri veritabanı satışları ve %9'u yetkisiz ağ erişimi satışlarından oluşuyor.
- E-ticaret, bankacılık ve sigortacılık en çok etkilenen sektörler arasında.
- Suç faaliyetlerinin arkasında olduğuna inanılan ilk 10 fidye yazılımı grubu, son üç yılda yaklaşık 5,2 milyar dolar değerinde Bitcoin elde etti. Türkiye'yi hedefleyen en büyük fidye yazılımı grupları LockBit, Conti ve Xing.
- Coğrafi konumu nedeniyle Türkiye, Rusya-Ukrayna gerilimi gibi jeopolitik konularda etki kazanmak isteyen APT aktörlerinin hedefinde. Türkiye'de faaliyet gösteren önemli APT grupları arasında APT28, APT29, APT39 ve APT41 sayılabilir.
- SOCRadar, son 12 ayda milyonlarca tüketiciyi hedef alan toplam 42 bin 136 oltalama (phishing) saldırısı tespit etti.
- En yaygın olarak yararlanılan güvenlik açıkları CVE-2021-31206, CVE-2021-21985, CVE-2020-5902 ve CVE-2021-3064 oldu.
- Türkiye ~31Tbit/sn DDoS trafiği üretebiliyor ve bu oranla dünya genelinde 27. sırada yer alıyor.

Dark Web Tehditleri Yükselişte

Çeşitli bilgisayar korsanlığı araçları, dolandırıcılık yöntemleri ve satın alınabilecek çalıntı veri tabanları ile dark web, siber saldırıları başlatmak için bir sıçrama tahtası gibi işlev görüyor. Dark webde doğan siber tehditler, Türkiye'deki kuruluşları giderek daha fazla etkiliyor.



Şekil 1. DarkMirror Intelligence verilerine göre Türkiye'de en çok hedeflenen sektörler

SOCRadar'ın DarkMirror Intelligence hizmetinden toplanan verilere göre, Türk varlıklarını hedef alan 150'den fazla 30 tehdit aktörü listesi mevcut. Gönderilerin %22'si müşteri veritabanı satışları ve %9'u yetkisiz ağ erişimi satışlarından oluşuyor. Tehdit aktörleri tarafından listelenen bu gönderiler, finans, telekomünikasyon ve eğitim dahil olmak üzere çeşitli sektörlerden farklı kuruluşları etkiliyor.

158
Son bir yıldaki tehdit gönderi sayısı

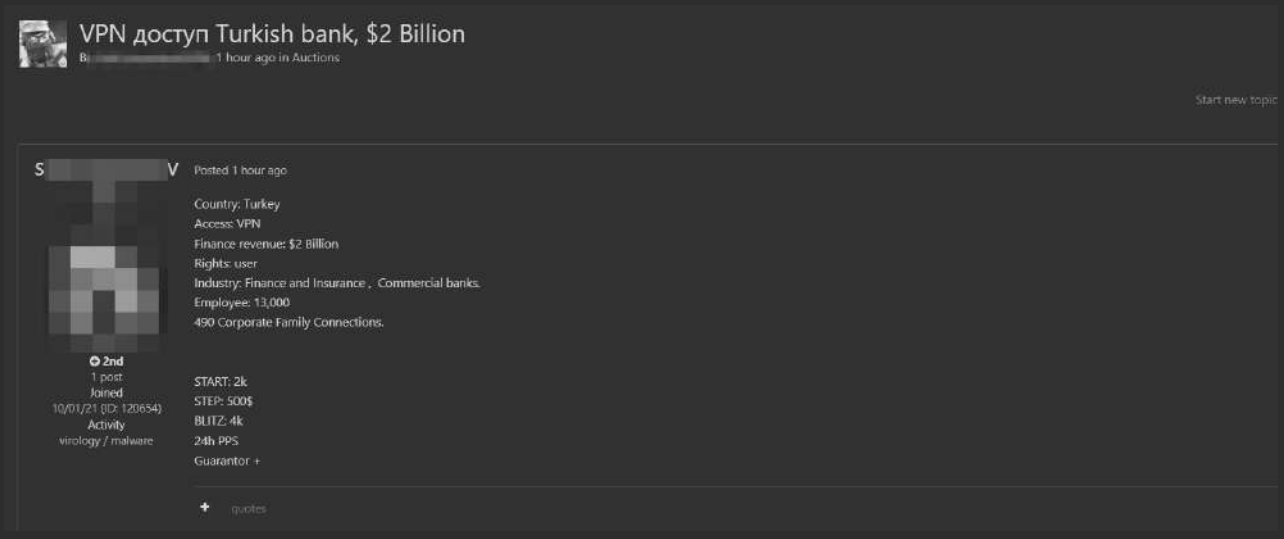
Finans | Eğitim
En çok hedeflenen sektörler

30
Dark webteki tehdit aktörü sayısı

Müşteri veri tabanları
En çok etkilenen tehdit kategorisi

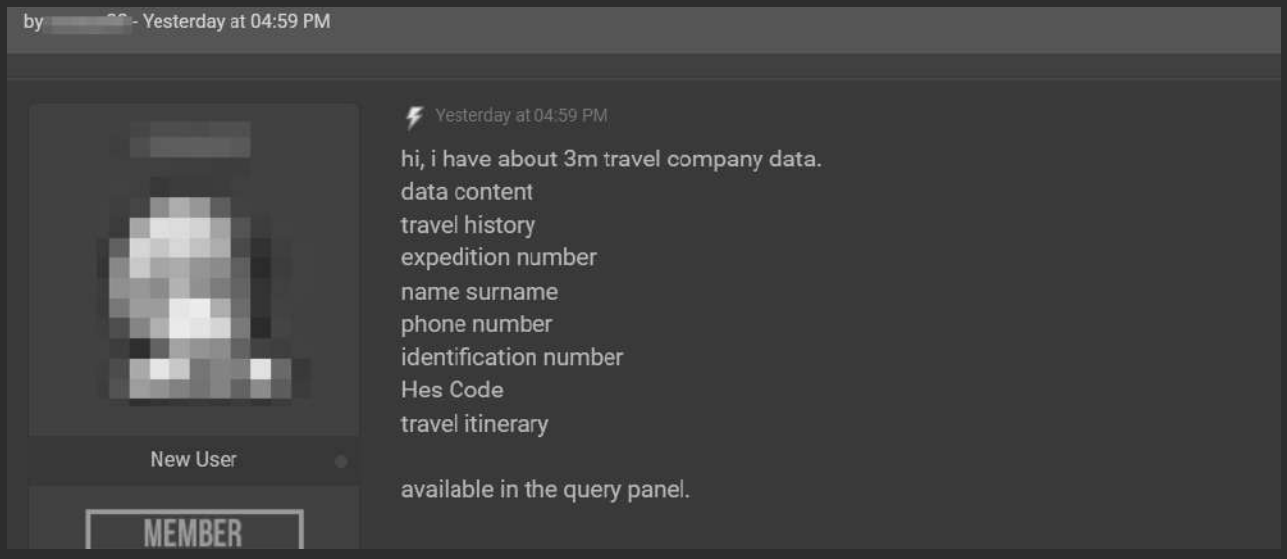
Yakın Zamanlarda Türk Firmalarına Yönelik Gerçekleşen Dark Web Faaliyetleri

13.000 çalışanı olan bir Türk Bankasına Yetkisiz VPN Erişimi Satışı Tespit Edildi:



- 10 Aralık'ta, SOCRadar tarafından takip edilen bir dark web forumundaki tehdit aktörü, iddiaya göre bir Türk finans kurumu için yetkisiz VPN erişimi satmaya çalıştı. Dark web satıcısı kurban organizasyonun 13 bin çalışan ve 2 milyar dolardan fazla gelire sahip olduğunu iddia ediliyor. Tehdit aktörü, 2.000 dolarlık bir başlangıç fiyatı ayarlayarak VPN erişimini açık artırmaya çıkardı.

Bir Türk Seyahat Şirketine Ait 3 Milyon Satırlık Müşteri Veritabanı Satımı:



28 Kasım'da, SOCRadar tarafından izlenen bir dark web forumundaki tehdit aktörü Türkiye'den büyük bir seyahat acentesinin müşteri veritabanını satmayı teklif etti. Aktörün paylaştığı listeye göre, alıcı, 3 milyon satırdan oluşan veritabanı içerisinde kullanıcıların kimlik detayları, seyahat geçmişleri ve yolculuk güzergahlar dahil olmak üzere çeşitli veriler bulunuyordu. Tehdit aktörü ayrıca, potansiyel alıcıların geçerliliği kontrol etmek için veritabanını sorgulayabileceğini de iddia etti.

Türkçe Konuşan Yeraltı Forumlarının Sayısı Artıyor

Türkçe paylaşımların bulunduğu yeraltı bilgisayar korsanlığı/dolandırıcılık forumları, siber tehdit unsurlarının anonim olarak yeni kişilerle iletişim kurmaları ve reklam vermeleri için olanak sağlıyor. Tehdit aktörleri, bu forumlar ve mesajlaşma uygulamaları aracılığıyla kimlik bilgileri doldurma dahil olmak üzere çeşitli saldırılar için bilgisayar korsanlığı araçlarını değiş tokuş ve takas etme imkanı buluyor.

E-Ticaret, Bankacılık & Finans ve Sigortacılık Türkiye'de siber tehditlerden en çok etkilenen sektörler arasında yer alıyor. Bunun yanında, SOCRadar CTIA ekibi yaptığı araştırmada, Telegram, ICQ ve Discord gibi meşru platformlara taşınan Türkçe konuşan hacker aktivitelerinde bir artış gözlemledi.

Türkçe Konuşan Yeraltı Hacker Topluluklarının Paylaşımlarından Bazı Örnekler

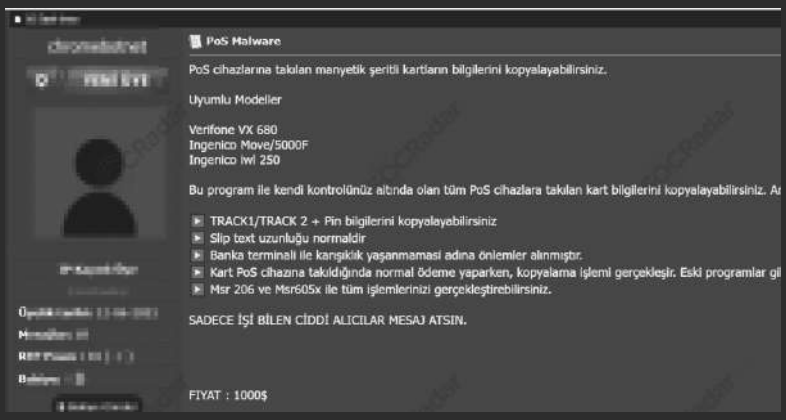
Türk Dark Web Forumunda Satılık Hizmet Olarak 'Stealer Virüsü':

Gelecekteki siber saldırıları kolaylaştırmaya yardımcı 'satılık hizmet olarak Stealer Virüsü'nü açıklayan bir dark web gönderisi

Rakiplerin İşlerini Aksatmak İçin Satılık Tam Teşekküllü DDoS Saldırısı:

Rakipleri bozguna uğratmak için bir araç olarak tanıtılan satılık bir DSoS saldırısı.

Satılık POS Uyumlu Kredi Kartı Klonlama Yazılımı:



POS cihazlarından ödeme verilerini kopyalayıp çalmak için geliştirilen kötü amaçlı yazılım programı.

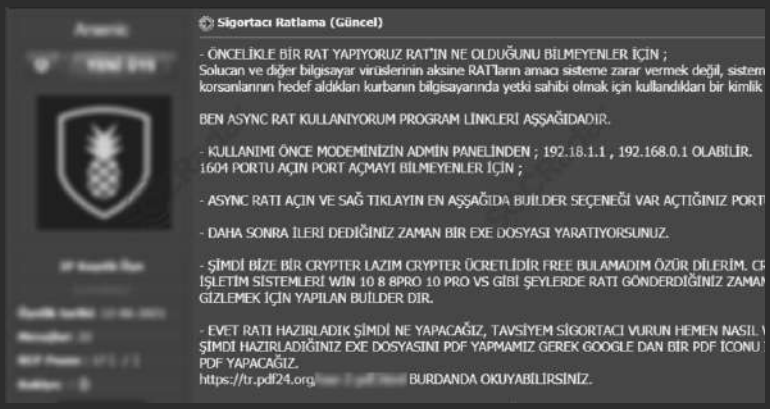
35 Milyon Türk Vatandaşının PII Verilerinin Satıldığı İddiası:

MERNİS verileri, vatandaşların eksiksiz adres ve kimlik bilgilerini içerdiği için değerli. Bu durum sosyal mühendislik saldırıları için alan açıyor.

Tehdit Aktörleri Kimlik Doldurma Trendine Ayak Uyduruyor:

Bir tehdit aktörü, çevrimiçi bir medya platformunun müşterilerine ait 20 binden fazla kimlik bilgilerine (kullanıcı adı ve şifre) eriştiğini iddia etti. Aktörün bu verileri, gelecekteki olası satışlar için itibar kazanmak için ücretsiz olarak sunduğu ortaya çıktı.

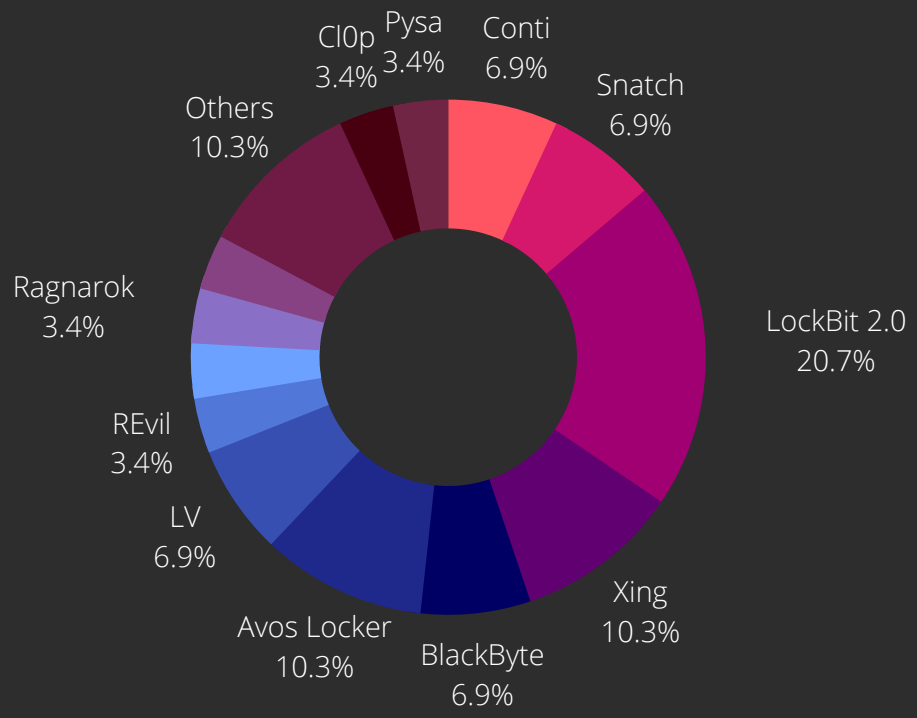
Sigorta Şirketlerini Hedefleyen Uzaktan Erişim Aracı Yöntemi Tespit Edildi:



Bir tehdit aktörünün bu listesi, AsyncRAT'ın ayrıntılı bir tanımını sunar ve Türkiye'de faaliyet gösteren sigorta komisyoncularını ve acentelerini hacklemek için nasıl kullanılabileceğini anlatır.

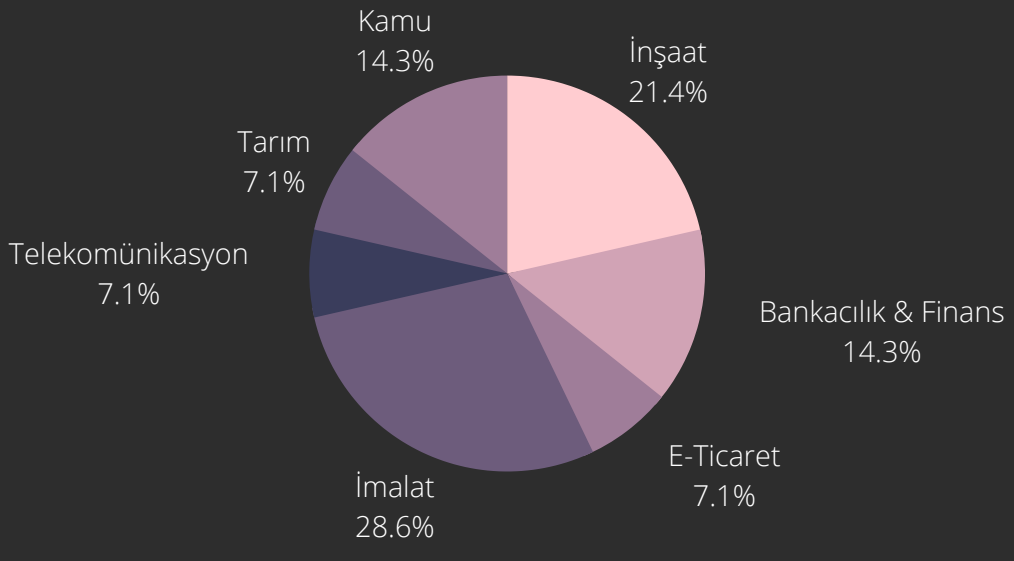
2021'de Fidye Yazılım Tehditleri Hızla Arttı

Fidye yazılımı (ransomware) saldırıları 2021'de manşetlerde sık sık kendine yer buldu. Türkiye'deki fidye yazılımı saldırılarının arkasındaki ilk 10 fidye yazılımı grubunun, son üç yıldaki hasılatı yaklaşık 5,2 milyar dolar oldu. Türkiye'de hizmet gösteren birçok küresel firma da bu yıl önemli fidye yazılımı saldırılarıyla karşılaştı ve bu da işletmelerin sekteye uğramasına neden oldu.



Şekil 2. 2021 yılında Türkiye'yi hedefleyen fidye yazılımı gruplarının faaliyet gösterme oranlarına göre dağılımı

2021'in son üç ayında fidye yazılımı saldırılarındaki artış hızlandı. Endişe verici bir şekilde, Türkiye'yi hedefleyen fidye yazılımı gruplarının faaliyetleri Haziran'dan Aralık 2021'e üç kattan fazla arttı. SOCRadar DarkMirror'da yer alan verilere göre "İmalat ve Finans" en çok hedeflenen sektörler arasında yer aldı.

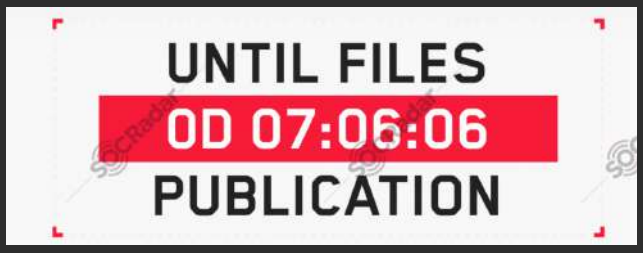


Şekil 3. 2021'de fidye yazılım gruplarının Türkiye'de hedeflediği sektörler

Türkiye'yi Hedef Alan En Büyük Fidye Yazılım Grupları

LockBit

- ”Hizmet olarak fidye yazılımı” (RaaS) operatörü.
- Şifreleme hızı ve genel işlevsellik açısından en iyi tasarlanmış lockerlardan biri.
- Son zamanlardaki saldırdığı firmalar arasında Schneider Electric, Accenture ve Bangkok Airways bulunuyor.



Conti

- Rusya dışında faaliyet gösteren bir ”Hizmet olarak fidye yazılımı” (RaaS) operatörü
- Grup, ilaç da dahil olmak üzere çok çeşitli sektörlerde Türk şirketlerine yönelik yüksek profilli saldırılar gerçekleştirmesiyle biliniyor.
- İddiaya göre Conti ile ilgili bir taktik metni, Conti tarafından hedef alınan bir kuruluş tarafından Eylül 2021'de yayımlandı.

Xing

- "Xing”" Mandarin dilinde "yıldız" anlamına geliyor.
- Grup, eskiden faaliyet gösteren “MountLocker/Avaddon” fidye yazılımı grubunun isim değiştirmesi olarak değerlendirildi.
- Hedeflenen firmalar arasında Türkiye’den gıda, imalat ve lojistik şirketleri bulunuyor.
- Ağlar arasında solucan kurmak için Enterprise Windows Active Directory API'lerini kullanıyorlar.

Türkiye'yi Hedef Alan APT Grupları

Türkiye'den firmalar, çeşitli amaçlarla hareket eden becerikli APT gruplarının hedefi olmaya devam ediyor. APT grupları, finansal avantaj elde edebilecek, stratejik süreçlere erişebilecek veya stratejik istihbarat toplayabilecek çok miktarda değerli bilgi ve varlığı ele geçirebileceği kuruluşları sıklıkla hedef alıyor

Coğrafi konumu nedeniyle Türkiye, Rusya-Ukrayna gerilimi gibi jeopolitik etki kazanmak isteyen bazı ulus-devlet aktörlerinin hedefine girebiliyor. Örneğin 2021 boyunca, ChamelGang gibi yeni APT gruplarının da Türkiye ve komşu ülkelerde güçlerini artırdığı gözlemlenirken, "enerji, kritik kamu altyapıları ve finans" çekici görülen ilk üç sektör arasına giriyor.

Türkçe Deep Web Forumlarında Faaliyet Gösteren Önemli APT Grupları

APT41

Son görülme
Aralık 27, 2021

APT28

Son görülme:
Aralık 25, 2021

APT39

Son görülme:
December 27, 2021

APT29

Son görülme:
December 25, 2021

Yakın Tarihli APT Faaliyetlerinin Bir Özeti

Yeni APT Grubu “ChamelGang”, Tedarik Zinciri Saldırılarıyla Türkiye'yi Hedefliyor:

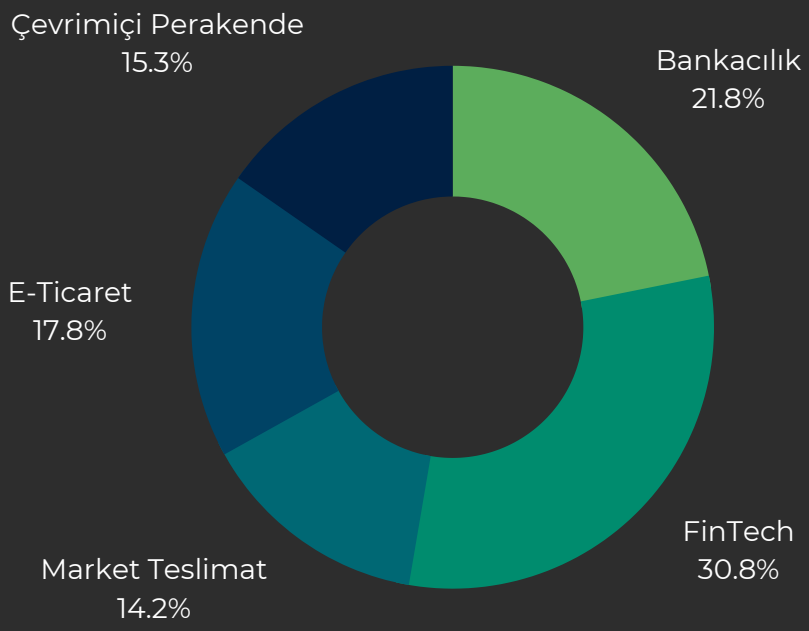
2021'de araştırmacılar, Türkiye, Amerika Birleşik Devletleri, Rusya ve Japonya dahil olmak üzere çeşitli ülkelerde yakıt, enerji, kamu ve havacılık sektörlerini hedefleyen yeni bir APT grubu tespit ettiler. Soruşturmalar, grubun Microsoft Exchange Sunucularında ProxyShell ve RedHat JBoss Uygulama Sunucusu platformunda CVE-2017-12149 gibi güvenlik açıklarından yararlandığını ortaya çıkardı. Buna göre saldırganlar, ilk erişimi kazandıktan sonra, DoorMe adlı arka kapının değiştirilmiş bir sürümünü yüklüyor ve gizleme amacıyla meşru IIS sunucu modülleri olarak adlandırıyorlar. APT grubu ayrıca, Türkiye'deki kuruluşlar tarafından yaygın olarak tercih edilen Microsoft, GitHub ve McAfee gibi tanınmış teknoloji şirketlerinin taklit etmek için oltalama (phishing) domainlerini kaydettirip SSL sertifikalarını kullandılar. Grup, bu saldırı aşamalarını bir yan kuruluşta gerçekleştirerek, güvenilir tedarik zinciri ağ kanallarından ödün vererek lider hedef kuruluşlara sızmayı amaçladı.

Siber Casusluk Grubu “Gelsemium”, Karmaşık Kötü Amaçlı Yazılımlarla Türkiye’den Bazı Kuruluşları Hedef Alıyor:

Haziran 2021'de araştırmacılar, Gelsemium isimli siber casusluk grubunun Doğu Asya ve Orta Doğu'daki hükümetleri, elektronik şirketlerini, üniversiteleri ve dini kuruluşları hedef alan yeni kampanyalarını ortaya çıkardı. 2014'ten beri aktif olduğu bilinen Gelsemium, “Gelsemine” adlı yeni modüler kötü amaçlı yazılımını analiz ederek daha karmaşık operasyonel tekniklerin ve daha yüksek düzeydeki C++ becerilerini gerçekleştirebiliyor. Uzmanlar, grubun dünya çapında 150 milyondan fazla kullanıcısı olan BigNox Android Emulator'ın bir parçası olan Nox Player'a yönelik tedarik zinciri saldırısının arkasında olduğuna inanıyor. Grup, MS Exchange'de (CVE-2020-0688) bir RCE güvenlik açığından yararlanıyor. Grup ayrıca oltalama e-postalarıyla kötü amaçlı belgeler dağıtıyor (örn. özgeçmişler). Grubun bir diğer tipik özelliği ise normal alan adlarından daha ucuz olan kötü amaçlı yazılım komut ve kontrol sunucuları için Dinamik DNS alan adlarını yaygın olarak kullanması.

Türkiye'deki Oltalama (Phishing) Tehditleri

Tehdit aktörleri, Türkiye'de yeni doğan ve hızla büyüyen çevrimiçi yemek siparişi, e-ticaret ve yeni nesil bankacılık uygulamalarının sağladığı yüksek mobil erişime çabuk adapte olmuş görünüyorlar. Söz konusu şirketlere kayıtlı kullanıcıların hassas bilgilerini çalmak ve dahili sistemlere ilk erişim sağlamak için bu şirketleri taklit eden yüzlerce oltalama domaini günlük olarak kaydedildi.



Şekil 4. 2021 boyunca SOCRadar'ın "Phishing Domain Alert Generation" (Oltalama Etki Alanı Uyarısı) verilerine göre siber tehdit aktörlerinin en sık hedeflediği sektörler.

Digital Risk Protection hizmeti ile büyük kuruluşların ve bankaların ilk tercihi olan SOCRadar, son 12 ayda milyonlarca tüketiciyi hedefleyen toplam 42 bin 136 kimlik avı saldırısı tespit etti ve böylelikle otomasyonla çalışan, taklit domainlerini, mobil uygulamaları ve sosyal medya hesaplarını kullanarak binlerce kötü amaçlı altyapıyı engelledi.

42,136

2021 boyunca tespit edilen oltalama saldırısı sayısı

10 Milyon+

Türkiye'deki internet kullanıcılarının, yayından kaldırmalar yoluyla hedefi olmaktan korunduğu toplam oltalama saldırısı sayısı

FinTech

Oltalama saldırılarının en çok hedef aldığı sektör

Oltalama Saldırılarının Yaygın Olarak Hedef Aldığı Dijital Sektörler

Sosyal Medya

Saldırganın amacı

Kötü amaçlı yazılımları dağıtmak ve bireylerin sosyal medya giriş bilgilerini çalmak.

Bulut / Webmail

Saldırganın amacı

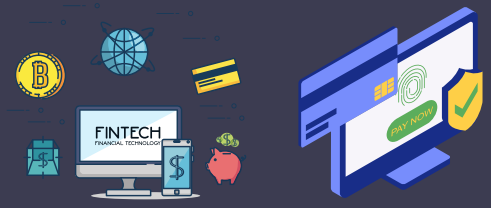
Kurbanların iletişim kanallarını ele geçirmek amacıyla kurumsal e-posta kimlik bilgilerini çalmak.

Perakende / E- ticaret

Saldırganın amacı

Tanınmış markaların popülaritesinden yararlanmak ve dolandırıcılık amaçlı e-ticaret faaliyetlerinde kullanmak üzere tüketicilerin/ şirketlerin kimlik bilgilerini ve diğer kişisel bilgilerini (PII) çalmak.

FinTech / Bankacılık



Saldırganın amacı

Türkiye'deki mobil erişim arttıkça genç nüfus arasında giderek yaygınlaşan yeni nesil finans ve bankacılık uygulamalarından tüketicilerin/işletmelerin giriş hesaplarını kazanç amaçlı çalmak veya bunları yasa dışı işlemlerde kullanmak.

Kritik Varlık Etkileri ve Güvenlik Açıkları

2021'in son günlerinde, yaygın olarak kullanılan Java tabanlı loglama kütüphanesinde Log4j'de bir güvenlik zafiyeti CVE-2021-44228 olarak adlandırılan #log4shell) keşfedildi. Son derece kritik bu güvenlik açığı, güvenlik cihazları da dahil olmak üzere çok sayıda kurumsal yazılım uygulamasını etkiledi. Saldırganlar, inanılmaz derecede kolay istismar edilebilen bu kusuru bulmak ve kullanmak için hemen interneti taramaya başladı.

Fidye yazılımı grubu Khonsari ve APT grupları da Log4j'deki güvenlik açığından yararlandı. SOC ekipleri, zafiyetten etkilenen sunucuları tespit etmeye çalışırken, SOCRadar Analistleri, Türkiye'deki kuruluşların, istismar edildiği bilinen internete açık sunuculardaki güvenlik zafiyetlerini gözardı etmemelerini tavsiye ediyor.

Türkiye'de internete açık sunucular risk altında | CVE Kimliği | CVSSv3

(Yalnızca en yaygın olarak yararlanılan güvenlik açıkları listelenmiştir.)

1924	Microsoft Exchange Server	CVE-2021-31206 #ProxyShell#UnauthRCEvulnerability	CVSS: 9.2
190	VMware vCenter	CVE-2021-21985 #vSphere #PreauthRCEvulnerability	CVSS: 9.8
110	F5 BIG-IP TMUI	CVE-2020-5902 #F5Networks #RCE	CVSS: 10.0
852	Palo Alto Networks VPN	CVE-2021-3064 #GlobalProtect #RCE	CVSS: 9.8

Diğer Kritik Bulgular

47,354
Exim Mail Server

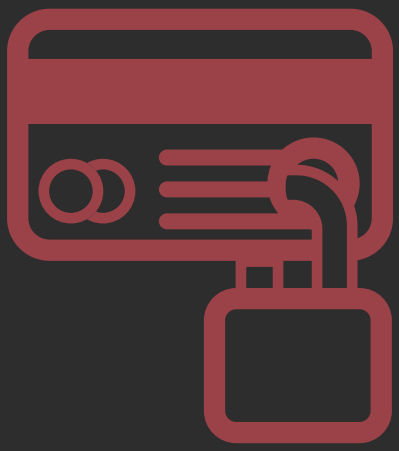
28,000
Open RDP 3389

1262
CVE-2014-0160
#Heartbleed

254
CVE-2019-0708
#BlueKeep

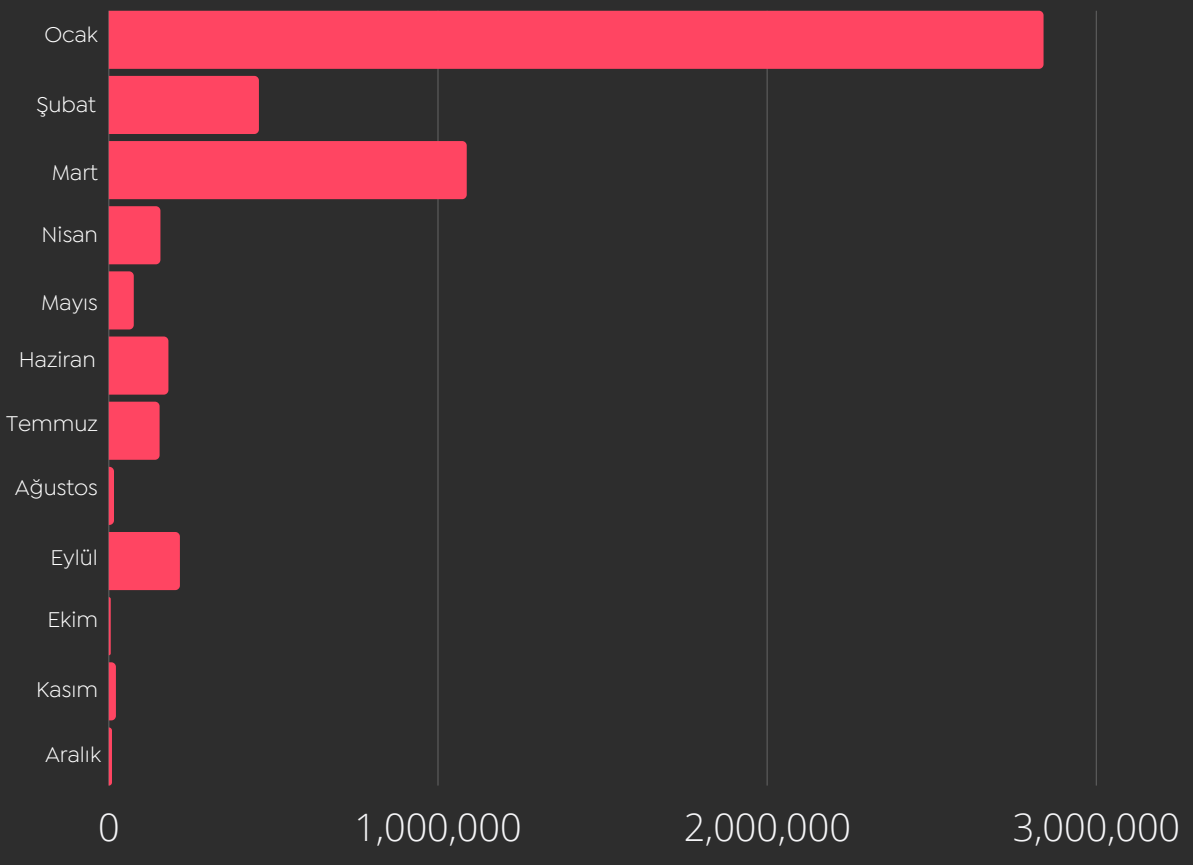
Kaynak SHODAN

Kimlik Bilgileri İstihbaratı



Sızan kimlik bilgilerinin kullanılması, tehdit aktörleri tarafından kullanılan en etkili ilk erişim vektörlerinden biridir. VIP'lere ait kimlik bilgileri, BEC saldırganları için faydalıdır. 2021 boyunca SOCRadar, dark web forumlrını ve marketplacelerini takip ederek düz metin parolalarla **5 milyardan fazla sızdırılmış** oturum açma verisini keşfetti.

Aynı parolaların tekrar tekrar yeniden kullanılması, çift taraflı doğrulama (2FA) mekanizmalarının eksikliğiyle birleştiğinde, sonuç yıkıcı olabiliyor. Fidye yazılımı aktörleri de dahil olmak üzere siber saldırganlar, böylesi elde edilmesi kolay dijital kimlikleri arıyorlar. Türkiye'nin mevcut risk durumuna ilişkin istatistikler ise aşağıdaki gibi:



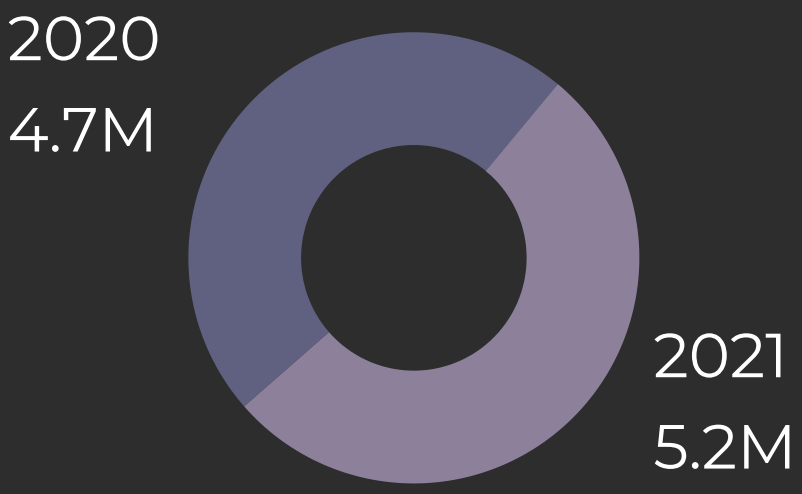
Şekil 5. 2021'de Türkiye ile ilgili tespit edilen kimlik bilgilerinin aydan aya değişim sayısı

BLACKMARKET İSTATISTİKLERİ

41.4Bin
Satılık Türk botlarının sayısı

1Milyon
Satılık botların toplam sayısı

Genesis ve benzeri blackmarketler, yüzde ikilik oranının Türkiye'den geldiği RedLine gibi kötü amaçlı yazılımların etkilendiği bot cihazlarının dijital kimliklerini satın almak için gerekli bilgileri edindikleri deep web caddeleri olan blackmarketlere örnek olarak verilebilir.



Şekil 6. SOCRadar, yalnızca 2021'de Türkiye ile ilgili 5,2 milyon çalıntı kimlik bilgisi keşfetti ve bu, 2020'de tespit edilen toplam kimlik bilgisinden 4,7 milyon daha fazlaydı.

5.2 Milyon
Toplam sızdırılmış kimlik bilgisi
Country code TLDs: com.tr | gov.tr | org.tr | mil.tr | net.tr

108.169
Kamu kurumlarından sızdırılmış kimlik bilgisi

DDoS I “Başkaları İçin Risk”

Küresel internet ekosistemi yıkıcı DDoS saldırılarına karşı savunmasızdır. Saldırganlar, her büyüklükteki kuruluşa karşı yıkıcı DDoS saldırılarını güçlendirmek için protokol bağımlılıklarıyla bu bağlantıdan yararlanarak finansal kayıplara ve tüm internet ekosistemini etkileyen hizmet kesintilerine neden olabilmekte.

DDoS saldırılarını durdurmak zor görünebilir; ancak, kolektif bir "başkaları için risk" zihniyeti, küresel düzeydeki riskleri azaltmamıza yardımcı olabilir. Cyber Green Initiative tarafından sağlanan küresel risk durumu verilerine göre, Türkiye ~31Tbit/sn DDoS trafiği üretebilmekte ve bu değerle dünya genelinde 27. sırada yer alıyor.

Protocol	Bandwidth Amplification Factor
DNS	28 to 54
SNMPv2	6,3
SSDP	30,8
CHARGEN	358,8
NTP	556,9

Şekil 7. Ülkelere göre toplam potansiyel DDoS bant genişliğinin ısı haritası görünümü

Veri Kaynağı: CyberGreen

31 TBit/Sec

Türkiye | Toplam DDoS Potansiyeli

97,977
Open Recursive DNS

9,643
Open SNMP

48,595
Open NTP

92
Open CHARGEN

1,043
Open SSDP

SOCRadar®

SOCRadar, Genişletilmiş Tehdit İstihbaratı, Dijital Risk Koruması ve Harici Saldırı Yüzey Yönetimi hizmetlerini bir arada sunan bir siber güvenlik platformudur. Ücretsiz olarak sağlanan hizmetleriyle müşterilerinin muhtemel siber tehditlere karşı proaktif olarak kendilerini savunmalarına yardımcı olur.

BİZİ TAKİP EDİN!

BİZE ULAŞIN

info@socradar.io

+1 (571) 249-4598