SWORDSEC

2022
TÜRKİYE SALDIRI YÜZEYİ RAPORU

SWORDSEC

İÇİNDEKİLER

SWORDSEC

TÜRKİYE SALDIRI YÜZEYİ RAPORU

2022 İlk Çeyrek

Yönetici Özeti

Küresel siber güvenlik risklerinin arttığı, şirketlerin fidye yazılımlarına maruz kaldığı ve finansal/itibar zararlarına sebep olan siber saldırılar son zamanlarda artış göstermektedir. Bu raporda, 2022 ilk çeyrek için Türkiye FORTUNE 500 şirketin[1] (Listeye internet/yazılım şirketleri dahildir.) açık-kaynak istihbarat[2] metodolojileri ile potansiyel siber güvenlik riskleri değerlendirilmiş olup alınması gereken önlemler detaylarıyla açıklanmıştır. Şirketler aşağıdaki kriterlere göre değerlendirilmektedir:

- E-Posta Güvenliği (MX, SPF)
- Web Sunucular (Web teknolojileri, başlıkları, web sunucu tipleri)
- Aktif Zafiyetli Sunucular (en az bir CVE'ye sahip olan host'lar)
- Kritik Portlar ve Servisler (Veritabanları, SSH, RDP, VNC, Telnet, SMB)
- DNS Güvenliği (Tahmin edilebilir aktif subdomainler)

Şirketlerin kategorileri ve teknik bilgileri aşağıda gözlemlenebilmektedir.

39
SEKTÖR

518
FARKLI ŞİRKET

84.100
AKTİF SUBDOMAIN

14.478
TOPLAM AÇIK PORT VEYA AKTİF SERVİS

138
CLOUDFLARE DNS[3]

1 https://www.fortuneturkey.com/fortune500
2 https://tr.wikipedia.org/wiki/A%C3%A7%C4%B1k_kaynak_istihbarat%C4%B1
3 CloudFlare DNS kaydı keşfedilen 138 IPv4'ler taramalara dahil edilmemiştir.

TANIMLAR VE KISALTMALAR

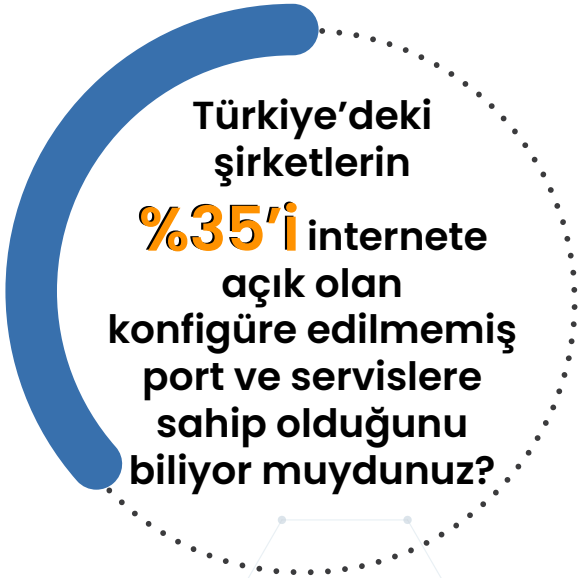
Port Nedir?

Port; internet üzerindeki cihazların bağlantı paketlerinin değiş tokuşunu sağlamak için kullanılan teknolojidir.
Portlar, temelde iki tip bağlantı türü kabul eder: TCP ve UDP. Bu bağlantıları kabul eden portlar "açık", bağlantı kabul etmeyen portlar ise "kapalı" olarak adlandırılır.

Açık Portlar Tehlikeli Midir?

Açık bir portun bulunması genelde tehlikeli kabul edilir ve kapatılması önerilir. Ancak portların açık olması internet üzerinde iletişimin kurulabilmesi için gereklidir. Açık bir portun bulunması genelde tehlikeli kabul edilir ve kapatılması önerilir. Bu birçok senaryoda geçerli olsa bile portların açık olması internet üzerinde iletişim kurulabilmesi için gereklidir.

Bahsi geçen açık portun üzerinde bağlantı kabul eden servisin düzgün konfigüre edilmemiş olması, bu servisin bilindik zafiyetlere sahip olması, sürümünün güncel olmaması bu portun güvenlik durumunu etkileyen faktörlerdir.



Saldırganlar Neden Açık Port Taraması Yaparlar?

Bir saldırgan, açık portu zararlı yazılım (exploit) çalıştırmak için kullanabilir. Saldırganlar bu işlem için öncelikle zafiyet bulması gerekmektedir. Zafiyeti bulmak için ise sistem üzerinde çalışan servisler hakkında detaylı bilgiye (sürümü, kullandığı protokol vb.) ihtiyaç duyar. Bu tür bilgilere herkese açık portları tarayarak elde ederler.

"Saldırı Yüzeyini ve güvenlik risk faktörünü etkileyen en önemli internet dijital varlıklarından biri port/servislerin konfigüre edilmeden internete açığa bırakmaktır."

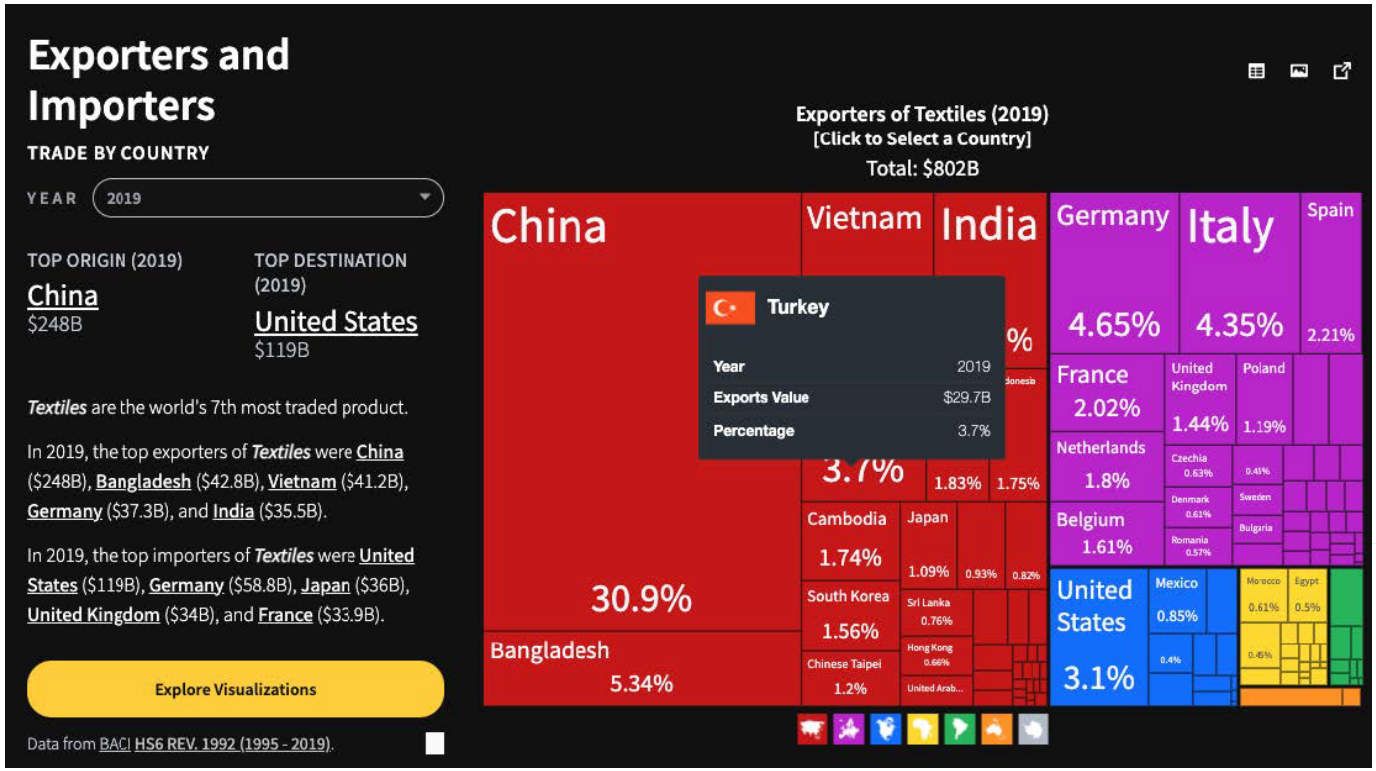
TANIMLAR VE KISALTMALAR

KISALTMA	AÇIKLAMA
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HTTP	Hyper Text Transfer Protocol
ISS	İnternet Servis Sağlayıcı
MX	Mail Exchange
NVD	National Vulnerability Database
SPF	Sender Policy Framework

ÖNE ÇIKANLAR

E-Posta Güvenliği: Rusya ile yaşanan sıkıntılardan dolayı MX (mail exchange) sunucuları Yandex kullanan çok sayıda önemli şirket keşfedilmiştir. Tavsiye olarak kendi mail sunucunuzu yapılandırmanızı tavsiye ederiz[4] veya GSuite sistemini kullanabilirsiniz.

Web Sunucular: En çok görülen siber saldırı türleri web saldırılarından gelmektedir. Günümüzde web teknolojileri çok geliştiği için saldırganların da iştahı burada kabarmaktadır. **Tekstil,** SSL sertifikası en çok olmayan sektör olarak saplantanmıştır.



2019

verilerine göre[5] **30 Milyar dolara** yakın ihracat potansiyeli olan **Giyim & Tekstil** sektörü, en kritik siber güvenlik zafiyetleri görülen sektör olmuştur.

EN İYİ/EN KÖTÜ SEKTÖR

4 https://ubuntu.com/server/docs/mail-postfix
5 https://oec.world/en/profile/hs92/textiles#exporters-importers

E-POSTA GÜVENLİĞİ

FQDN Nedir?

FQDN (Fully Qualified Domain Name) internet üzerindeki bir cihazın veya erişilebilir herhangi bir varlığın tam adresidir. Genel anlamda iki parçaya ayrılabilir: host adı ve domain. Örneğin mail.swordsec.com adresi için swordsec.com domain, mail kısmı ise host adıdır.

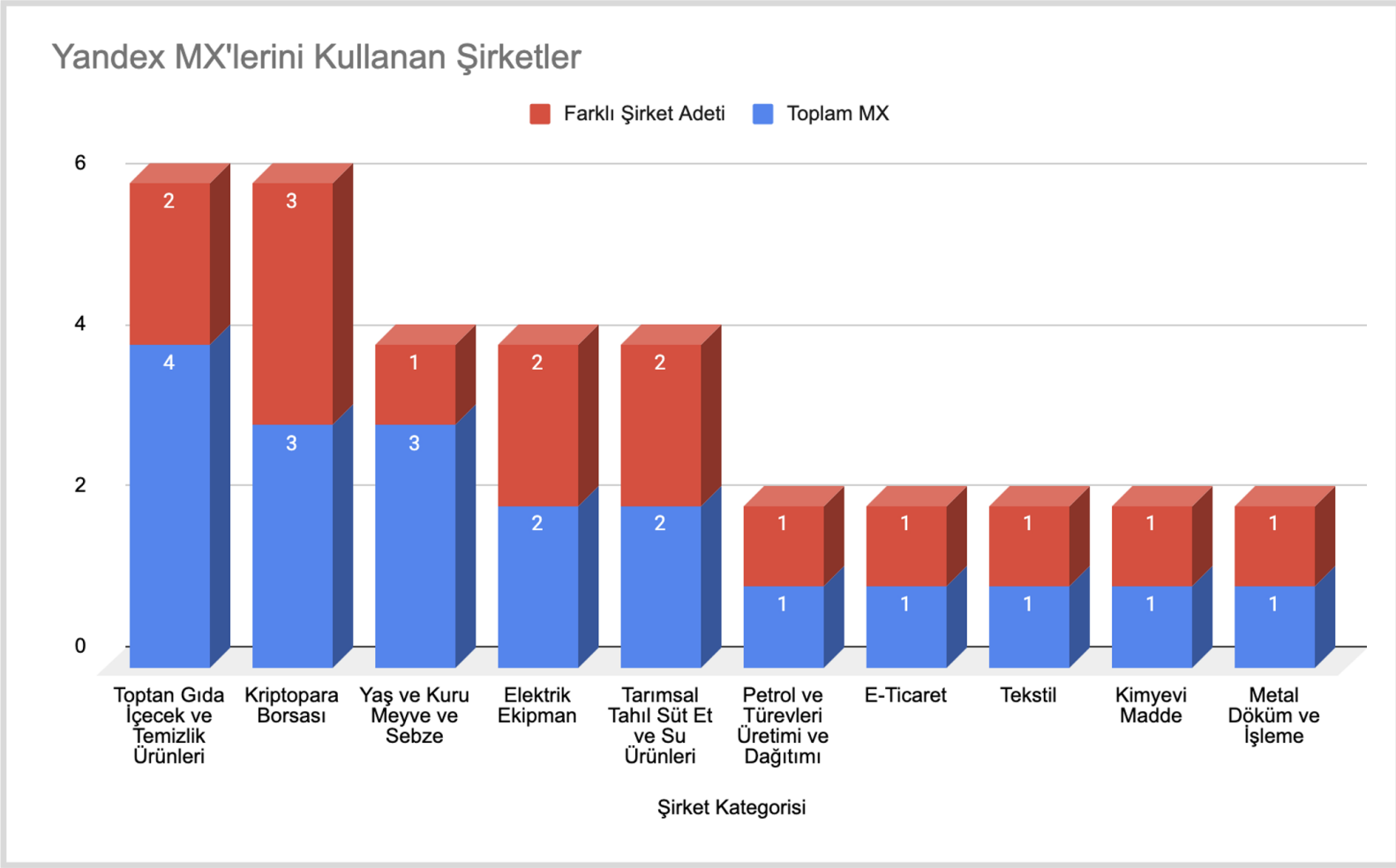
MX Nedir?

MX (mail exchange) kayıtları mail bağlantılarını kabul edecek mail sunucusunu gösterir. Bu kayıtlar bulunmazsa mail alıp yollanamaz.

Farklı FQDN adresleri aynı MX sunucusuna sahip olabilir. Tabloda mail sunucuları aynı olan FQDN adetleri listelenmiştir.

MX	FQDN Adeti	MX	FQDN Adeti	MX	FQDN Adeti
mx1.dsv.c3s2.iphmx.com	58	mxbounce-2.euromsg.net	11	antispam2.ihs.com.tr	6
mx2.dsv.c3s2.iphmx.com	57	mxbounce-1.euromsg.net	11	mx-in03.natrohost.com	5
alt1.aspmx.l.google.com	19	mxb-00308d01.gslb.pphosted.com	9	mx-in03b.natrohost.com	5
alt2.aspmx.l.google.com	19	mxa-00308d01.gslb.pphosted.com	9	aspmx4.googlemail.com	5
aspmx.l.google.com	17	alt3.aspmx.l.google.com	7	mx.eemms.net	5
mx.yandex.net	16	alt4.aspmx.l.google.com	7	mail.****.com.tr	4
aspmx2.googlemail.com	12	antispam1.ihs.com.tr	6	mxb.mailgun.org	4
aspmx3.googlemail.com	12	inbound-smtp.eu-west-1.amazonaws.com	6	mxa.mailgun.org	4

E-POSTA GÜVENLİĞİ



(Toplam MX adeti bir şirketin tüm subdomainlerinde görülen %yandex% MX'lerini kapsamaktadır.)

SPF Kaydı alıcı tarafındaki sunucu SPF kontrolü yapıyorsa, DNS kaydı içerisinde tanımlanan IP adresleri ve IP blokları dışından gelen istekleri kabul etmemesi ve yasal olmayan gönderimleri engellemesidir. Rapor sonuçlarına göre SPF kaydının en çok görülen şirketler "E-Ticaret" sektöründe yer almaktadır. Yüzdesel olarak görülen sektör ise "Sıhhı Tesisat ve İklimlendirme" ve "Bilgi ve İletişim Hizmetleri"'dir.

SPF GÜVENLİĞİ

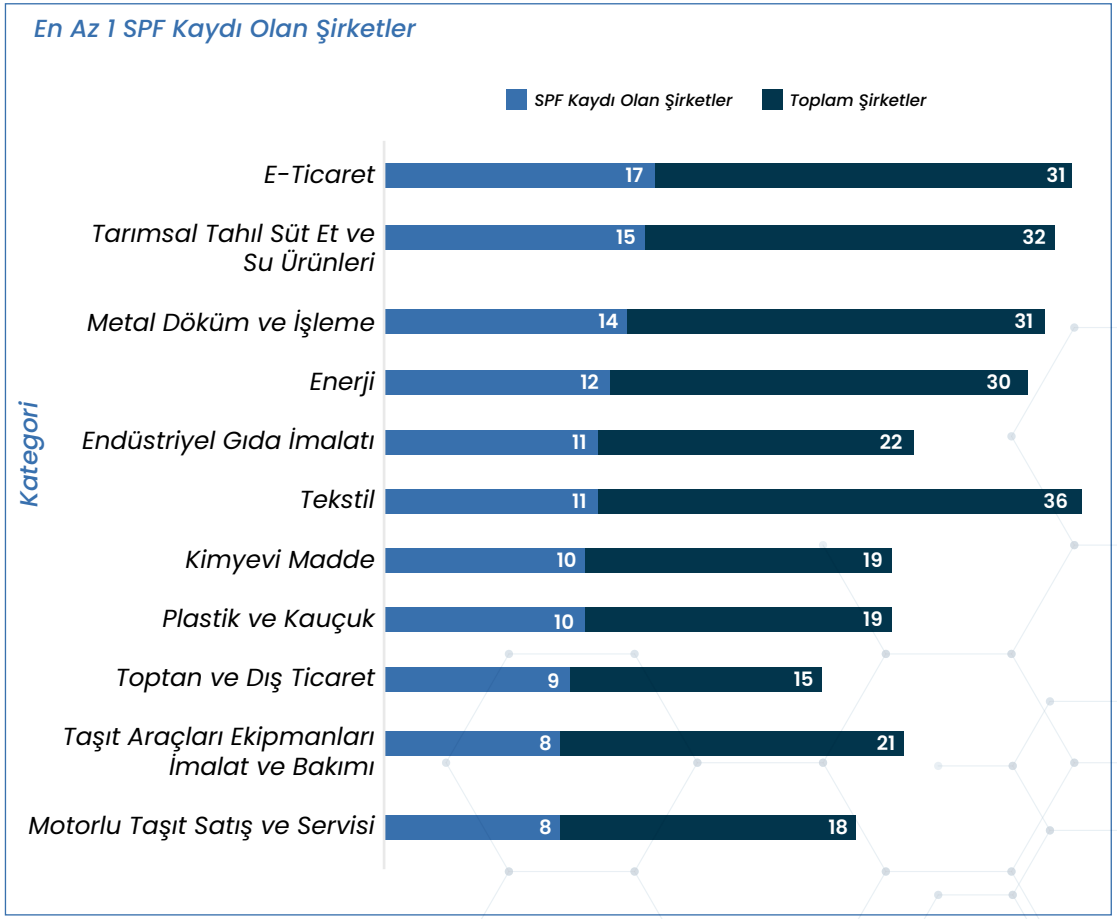
SPF Nedir?

SPF (Sender Policy Framework - Gönderen Politikası Çerçevesi), standart bir e-posta kimlik doğrulama yöntemidir. SPF, etki alanınızdan kimlerin e-posta gönderebileceğini kısıtlamak, etki alanı sahtekarlığını önlemek ve posta sunucunuzun, kullandığı etki alanından ne zaman bir ileti geleceğini belirlemesini sağlamak için DNS sunucularınızı güçlendirir.

SPF e-posta güvenliğinde tam bir güvenlik sağlamasa da güvenlik açısından faydalıdır. Örneğin, SPF kaydı ISS'ler(İnternet Servis Sağlayıcı) için ek bir güven sinyali sağlar. Bu, e-postalarınızın doğrudan kullanıcıların spam kutusu yerine posta kutusuna ulaşma şansını artırır.

SPF, "dönüş yolu" çalışma mantığını benimsemektedir. Bu çalışma mantığında öncelikle sistem, gönderen posta adresinin alan adını alır, daha sonra bu alan adına ait SPF kaydını inceler ve bu kayıtta gönderen IP sunucusuna izin verilip verilmediğine karar verir.

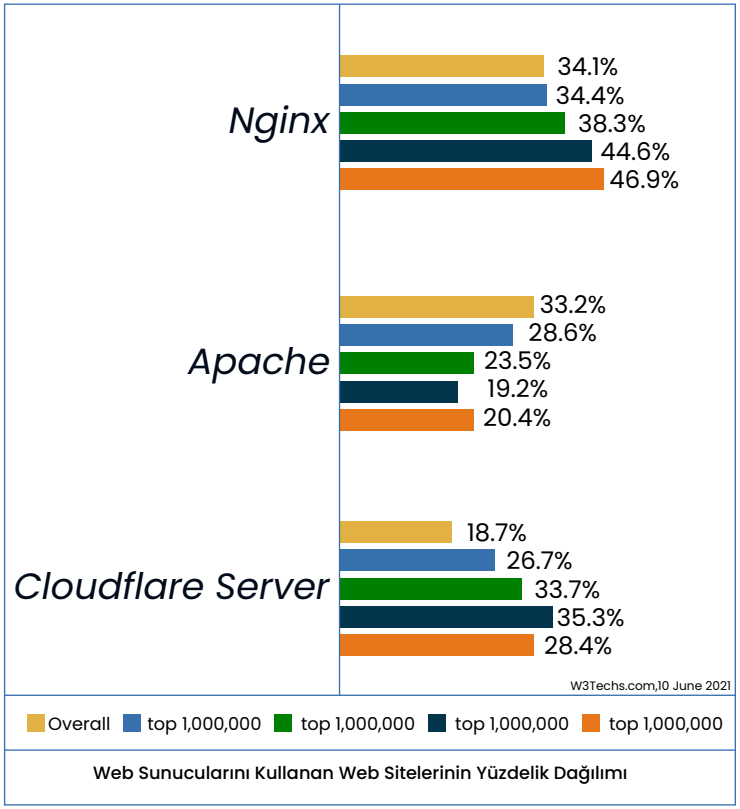
SPF kaydı için DNS'ye bir TXT girişi eklemek gerekir. Bu giriş ile izin verilen kayıtlar, e-posta göndermek isteyen sunucu bilgileri ile karşılaştırılır ve buna göre e-posta kabul edilir veya reddedilir. Bu kayıt sırasında dikkat edilmesi gereken en büyük konulardan biri ikinci bir TXT kaydının olmamasıdır. İkinci bir txt kaydına sahip olmak, sunucuların spf üzerinde başarısız olmasına neden olabilir.

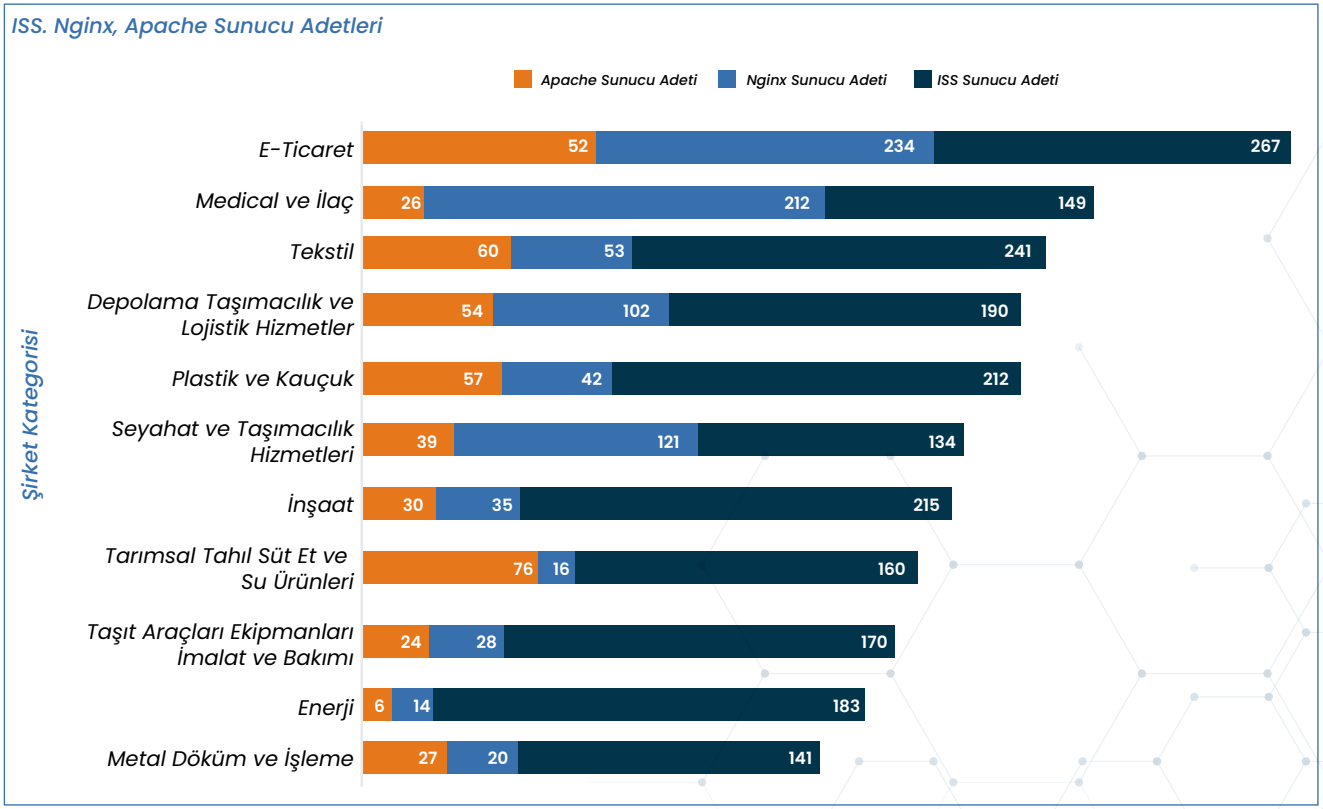


WEB SUNUCULAR

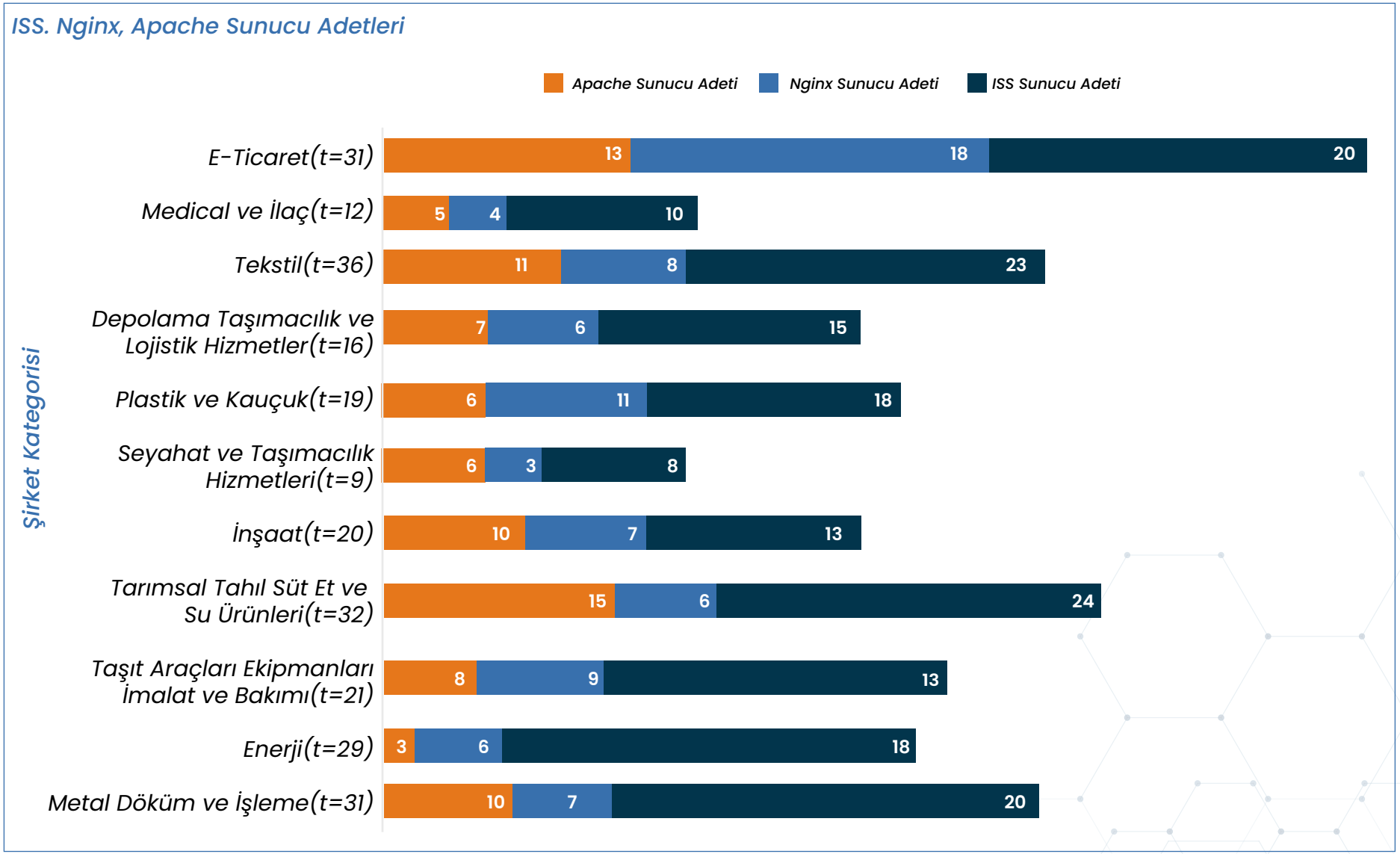
Web sunucusu internet üzerindeki diğer cihazlardan HTTP veya başka bir protokol ile bağlantı kabul eden cihaz ve yazılımdır.

Fiziksel anlamda web sunucusu internetteki diğer cihazlardan bağlantı kabul eder. Bu cihaz üzerinde web sunucu yazılımı bağlanan cihazların sunucu üzerindeki dosyalara erişimini kontrol eder. Her erişime açık web sitesinin bir web sunucu yazılımı vardır. Bu işi yapan birçok farklı yazılım bulunmaktadır fakat en yaygını ve popüleri olan NGINX'dir.





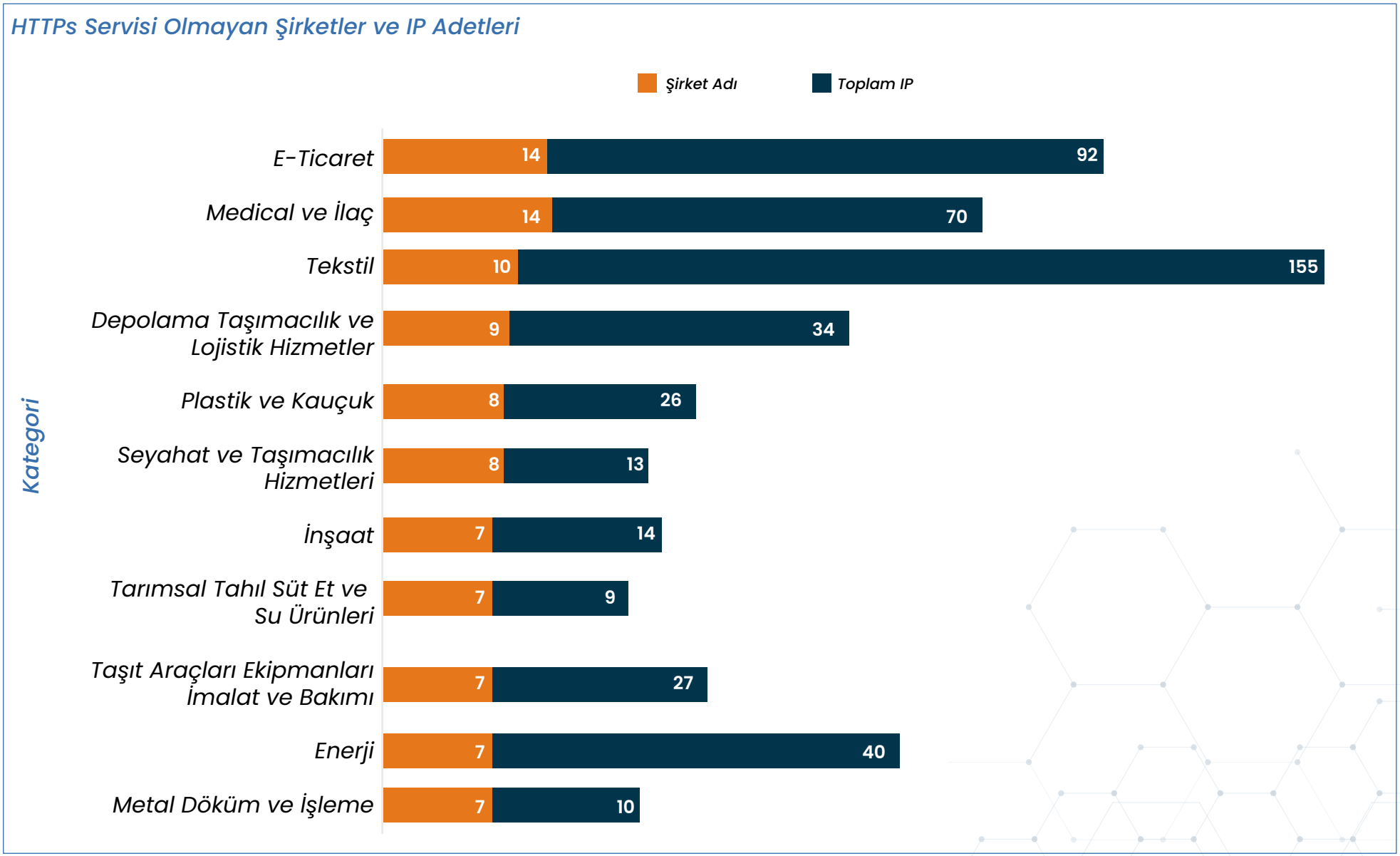
WEB SUNUCULAR



t=Şirket Adeti

* Bir şirket, birden fazla farklı web sunucularına sahip olabilir.

WEB SUNUCULAR



SAYFA BAŞLIKLARI

Sayfa başlıkları, sayfa içeriği hakkında bilgi içerir. Eğer bu başlık bir hata ile ilgiliyse saldırganların özellikle ilgisini çekecektir.

"Dorking" destekleyen çeşitli türde arama motorlarını kullanarak (Shodan, Google, Censys, SwordEye vb.) saldırganlar web sunucularının bilgi ifşa eden hata sayfalarını görebilirler.

BAŞLIK	ADET	ŞİRKET SEKTÖRÜ
ion admin	4015	Elektrik Ekipman
404 not found	3174	Plastik ve Kauçuk
cockpit	1556	Bilgi ve İletişim Hizmetleri
404 not found	1394	Bilgi ve İletişim Hizmetleri
microsoft azure web app - error 404	1372	Plastik ve Kauçuk
400 the plain http request was sent to https port	852	İnşaat
iis windows server	461	Toptan Gıda İçecek ve Temizlik Ürünleri
not found	335	Toptan Gıda İçecek ve Temizlik Ürünleri
menü	265	Elektrikli Ev Aletleri
404 not found	252	Taşıt Araçları Ekipmanları İmalat ve Bakımı
not found	166	Endüstriyel Gıda İmalatı
iis windows server	165	Endüstriyel Gıda İmalatı
- page not found. the specified page could not be found. (404)	136	Elektronik ve Telekomünikasyon

SAYFA BAŞLIKLARI

BAŞLIK	ADET	ŞİRKET SEKTÖRÜ
hostingstart-v2-02	118	Tekstil
403 - forbidden: access is denied.	98	Enerji
http status 400 – bad request	95	E-Ticaret
veritabanı hatası	82	İnşaat
not found	66	Taşıt Araçları Ekipmanları İmalat ve Bakımı
400 bad request	65	Seyahat ve Taşımacılık Hizmetleri
403 forbidden	61	Bilgi ve İletişim Hizmetleri
404 not found	56	E-Ticaret
[telco şirket ismi] ws	54	Bilgi ve İletişim Hizmetleri
not found	52	İnşaat
*** yem	47	Tarımsal Tahıl Süt Et ve Su Ürünleri
403 forbidden	41	Depolama Taşımacılık ve Lojistik Hizmetler
403 - forbidden: access is denied.	41	E-Ticaret
400 bad request	41	E-Ticaret
404 not found	40	Perakende Ticaret Mağazaları
not found	38	Tekstil

SAYFA BAŞLIKLARI

BAŞLIK	ADET	ŞİRKET SEKTÖRÜ
502 bad gateway	37	İnşaat
not found	36	Medikal ve İlaç
403 forbidden	33	E-Ticaret
the url you requested has been blocked	32	Bilgisayar Yazılım ve Büro Makinaları
400 bad request	31	Depolama Taşımacılık ve Lojistik Hizmetler
not found	31	E-Ticaret
not found	31	Enerji
400 the plain http request was sent to https port	31	Tekstil
sign in to your account	30	Toptan Gıda İçecek ve Temizlik Ürünleri
http status 404 – not found	28	Medikal ve İlaç
not found	27	Bilgisayar Yazılım ve Büro Makinaları
not found	27	Demir Çelik Ticareti
application server error	27	Makina ve Ekipmanları
301 moved permanently	27	Plastik ve Kauçuk
403 - forbidden: access is denied.	26	Taşıt Araçları Ekipmanları İmalat ve Bakımı
not found	25	Araç Kiralama Hizmetleri

SAYFA BAŞLIKLARI

BAŞLIK	ADET	ŞİRKET SEKTÖRÜ
not found	25	Elektrikli Ev Aletleri
server unavailable	25	Makina ve Ekipmanları
- page not found. the specified page could not be found. (404)	24	Yaş ve Kuru Meyve ve Sebze
apache tomcat	23	Elektrik Ekipman

Tüm şirketlerin aktif subdomainlerine HTTP 1.1 /GET isteği gidildiğinde aşağıdaki http durum kodları elde edilmiştir.

Güvenlik zafiyetleri konusunda önemli bilgi ifşası olabilecek HTTP durum kodlarından biri olan **500, 249** adet görülmüştür.

HTTP Status Kodu Neden Önemlidir?

HTTP durum kodları web sunucusuna yapılan isteklere göre verilen standartlaştırılmış cevaplardır. Eğer bu cevaplar konfigüre edilmezlerse web sunucu üzerinde çalışan yazılımın vereceği varsayılan cevap saldırganın sistem hakkında bilgi toplamasına büyük ölçüde yardım edebilir.

HTTP Durum Kodu	Adet	HTTP Durum Kodu	Adet
404	15123	409	3
400	1468	307	3
403	1200	596	2
503	987	308	2
500	**249**	402	2
401	236	501	2
502	67	504	2
303	49	405	1
204	23	410	1
429	10	525	1
521	8	417	1

SAYFA BAŞLIKLARI

HTTP başlık bilgisinde "**default**", "**test**", "**nginx**" ve "**iis**" içeren en çok görülen şirket aşağıdaki gibi saptanmıştır;

- Toptan Gıda İçecek ve Temizlik Ürünleri
- Endüstriyel Gıda İmalatı
- Plastik ve Kauçuk
- Bilgi ve İletişim Hizmetleri

Aşağıda tüm FQDN'lerde görülen "**default**", "**test**", "**nginx**" ve "**iis**" içeren başlıklar ve adetler mevcuttur.

Bir web sayfasının başlık (title) kısmının varsayılan (default) halinde olması, web sunucunun üzerinde çalışan yazılımın varsayılan cevabının gösterildiği anlamına gelir. Bu tür varsayılan sayfalardan saldırganlar sistem hakkında yıkıcı sonuçlar doğuracak bilgiler toplayabilirler.

Bu durumun önlenmesi için web sunucuda çalışan yazılıma göre konfigürasyon dosyası bulunmalı ve varsayılan sayfalar değiştirilmelidir.

SAYFA BAŞLIKLARI

BAŞLIK	Toplam FQDN Adet
iis windows server	789
web server's default page	106
iis7	26
default parallels plesk panel page	16
welcome to nginx!	16
default parallels plesk page	12
domain default page	10
iisarr-iis windows server	9
apache http server test page powered by centos	7
test page for the apache http server on red hat enterprise linux	6
apache2 ubuntu default page: it works	5
testing company	4
http server test page powered by centos-webpanel.com	4
iis 7.0 detailed error - 403.14 - forbidden	3
iis 10.0 detailed error - 403.14 - forbidden	3
iis windows server...	2
iis 10.0 detailed error - 500.24 - internal server error	2
apache2 debian default page: it works	2
leoni sfx (test)	2
php test	2
test	2
test store 19	2
visium load testing tool	2

CVE'LER

Aşağıdaki grafikte en az aktif 1 CVE'e sahip olan şirketlerin sektör grafiği yer almaktadır. Bulunan tüm yazılımların CPE'lerine göre eşleştirme yapılmıştır. Tüm şirketlerin aktif DNS A kaydındaki IPv4 adresleri ve FQDN'lerde web teknolojilerine göre CPE'ler alınmış ve CVE eşleştirmeleri yapılmıştır. Ayrıca aşağıda siber güvenlik risklerinin artmasına sebeb olan kritik servislerin portları (SSH, RDP, Telnet vb.) onlarca şirketlerde görülmüştür.

CVE (Common Vulnerabilities and Exposures), halka açık olarak sunulan bir zafiyet sözlüğüdür. Bu sözlüğün yaratılma amacı zafiyetler hakkında yapılan bilgi paylaşımını kolaylaştırmaktır. Bir CVE kaydı, zafiyet hakkında bir açıklama, bir zafiyet kimlik numarası ve en az bir halka açık referanstan oluşur.

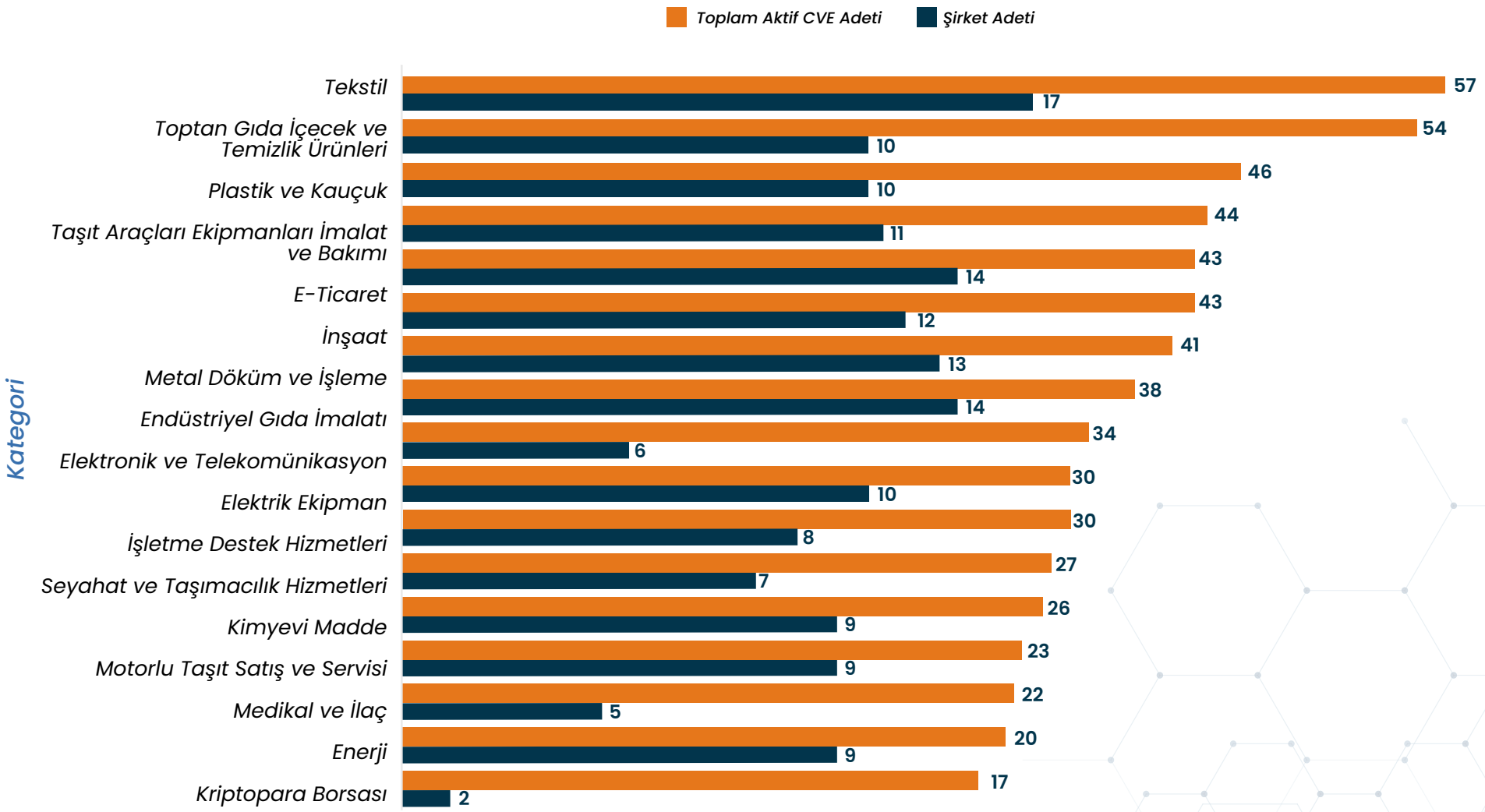
CVE, ABD İç Güvenliği DHS-United States Department of Homeland Security tarafından sponsorlanmakta olup, MITRE tarafından yürütülmektedir. CVE, aynı zamanda MITRE tarafından markalaştırılmıştır ve her hakkı MITRE'ye aittir.

CVE sözlüğü, halka açık olarak bedava bir şekilde sunulmaktadır ve bu sözlük üzerine belirli veritabanları kurulmuştur. Bu veritabanlarından en önemlileri arasında NVD (National Vulnerability Database - Ulusal Zafiyet Veritabanı) bulunmaktadır. NVD, CVE sözlüğü ile senkronize çalışan ve yine halka açık olarak bedava sunulan bir veritabanıdır. Bu veritabanında zafiyetler hakkında detaylı bilgiler bulunmaktadır.

En az 1 aktif CVE sahibi şirketler kategorilendirilmiştir. Taramalar sonucu bulunan yazılımların CPE'lerine göre eşleştirme yapılmıştır. Tüm şirketlerin aktif DNS A kaydındaki IPv4 adresleri ve FQDN'lerde web teknolojilerine göre CPE'ler alınmış ve CVE eşleştirmeleri yapılmıştır. Ayrıca aşağıda siber güvenlik risklerinin artmasına sebeb olan kritik servislerin portları (SSH, RDP, Telnet vb.) onlarca şirketlerde görülmüştür.

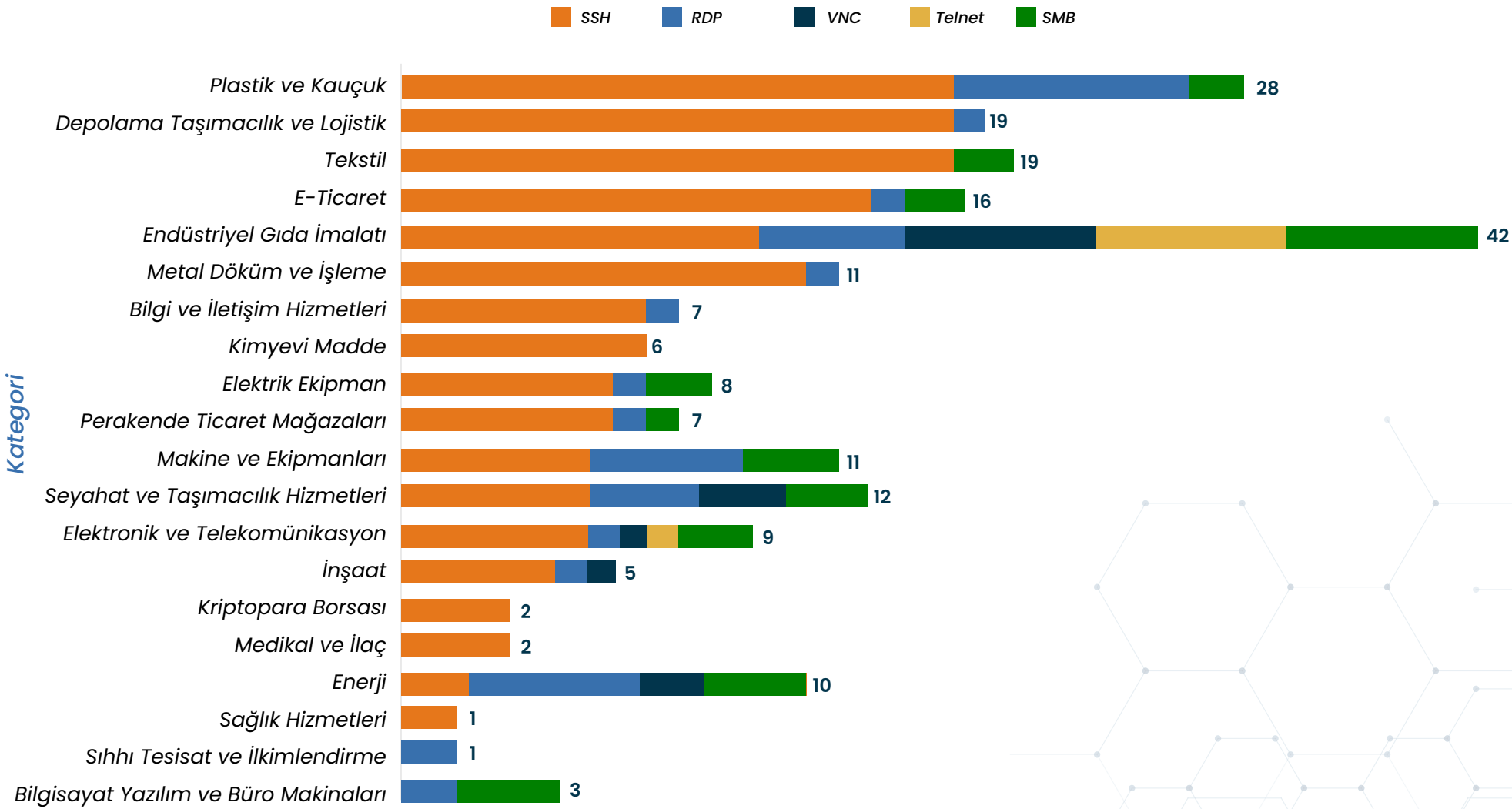
CVE'LER

En Az 1 Aktif CVE Bulunan Şirketler



CVE'LER

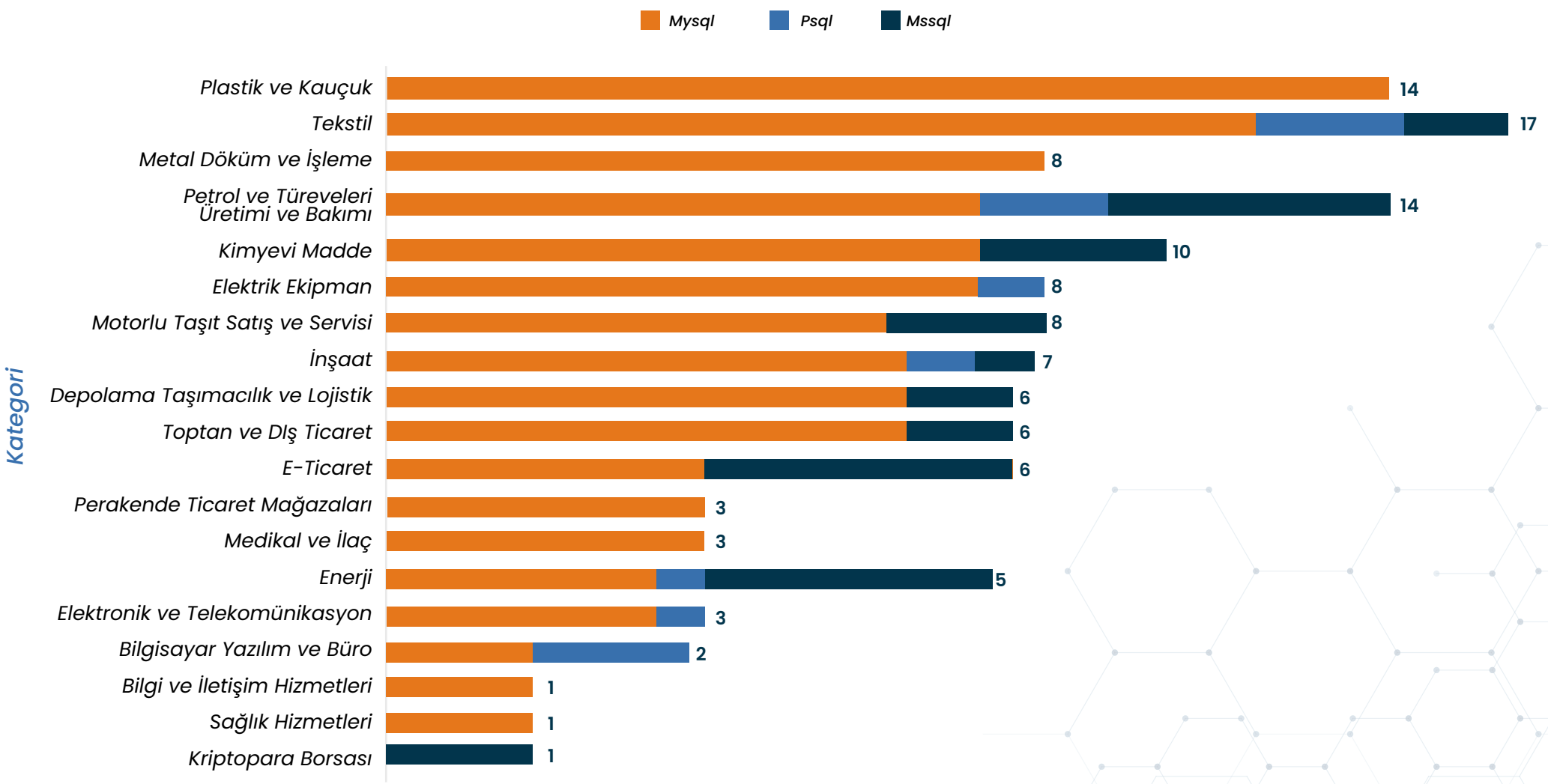
SSH, RDP, VNC, Telnet, SMB Servisleri



Grafikte görüldüğü gibi VNC portunu en çok kullanan "Gıda İmalat" sektörü olarak belirlenmiştir. Bu sektörde çoğunlukla **SCADA** sistemleri görülmektedir.

CVE'LER

Mysql, Psql ve Mssql Servisleri



SONUÇ

Saldırı yüzeyi; bir şirketin, sistemin veya kritik bir alt yapının, saldırganlara açık olan tüm alanıdır. Sistemlerin dijital izleri, dijital varlıkları, kullandıkları teknolojiler, versiyonlar gizli anahtarlar ve uygulama yolları saldırı yüzeyi ve risklerini artırır. Bu dijital varlıklar ve izler ne kadar çoksa tehdit faktörü de bir o kadar çoktur.
Saldırganlar sistemleri ele geçirmek için saldırı yüzeyine odaklanır. Sistemler hakkında edinebileceği her bir bilgi, hackerlar için oldukça değerlidir.

Veriler incelendiğinde Türkiye ekosistemindeki firmaların normalden yüksek saldırı yüzeyine sahip olduğu görülmektedir. Şirketlerde bilgi güvenliği yöneticileri sayılarının yetersizliği, bilgi düzeylerinin yüksek olmaması ve gerekli teknolojik araçların/ürünlerin/hizmetlerin alınmamasından dolayı bu durum ortaya çıkmaktadır.

Saldırı yüzeyinin azaltılması için izlenebilecek bazı önlemler olarak; web site ve uygulamalarının arka planda çalışan servislerinin dışarıya açık olmaması (veritabanı, bulut depolama vb), çalışanların güçlü şifre kullanması ve şifre güvenliği konusunda bilinçlendirilmeleri, sunucularda çalışan servislerin konfigürasyonlarının yapılması, sunucu üzerindeki eski servislerin kapatılması, sunucular üzerinde çalışan servislerin güncel olmaları, sunucunun bağlantılara verdiği cevaplarda bilgi sızıntısına sebep olabilecek başlık bilgilerinin kapatılması sayılabilir.

SwordEye, saldırı yüzeyini detaylı takip ederek risk ve potansiyel tehditleri en aza indirir. Sürekli ve düzenli taramalar sayesinde meydana gelen herhangi bir değişiklik kullanıcıya anında bildirilir ve çözüm önerileri verilir. SwordEye kullanıcıları veri ihlallerine karşı korunaklı, kendileriyle ilgili veri sızıntılarından hemen haberdar ve tüm dijital varlıklarının risk skorlaması ile siber tehditlere hazır olur.

DAHA FAZLA BİLGİ İÇİN;