2021 KÜRESEL HEDEFLİ FİDYE OPERASYONLARI: AKTÖRLER VE HEDEFLER

Süfyan Kadir KIVAM
Siber Güvenlik Araştırmacısı

Ersin ÇAHMUTOĞLU
Siber Güvenlik Araştırmacısı

Bu rapor, Adeo Siber Güvenlik Araştırma Ekibi tarafından yazılmıştır.

İçindekiler

ÖN SÖZ

Gelecekte karşılaşılacak siber saldırılar arasında ransomware (fidye) saldırılarının çok büyük bir orana sahip olacağı birçok analist tarafından ifade ediliyor. ADEO'nun siber güvenlik araştırmacıları tarafından hazırlanan bu raporda, sebep oldukları finansal kayıpların yanında bir çok kurum ve şirketin marka değerini de ciddi şekilde tehdit eden ve itibar kaybına sebep olan hedefli fidye saldırılarının 2021 yılı istatistikleri yer almaktadır. Bu saldırıları gerçekleştiren tehdit aktörlerine ait olan ve çoğunluğu "deepweb"de yer alan iletişim platformlarını inceleyerek kurbanları ve saldırıları gerçekleştiren grupların profillerini bir arada değerlendirdik. Gelecekte meydana gelebilecek olası saldırıların hangi profildeki şirketleri kurban olarak seçeceği ve kimleri hedef alacağı konusunda bir öngörüde bulunabilmek için elimizdeki istatistikleri ve davranış modellerini analiz ettik. Giderek daha çok artacağına inandığımız hedefli fidye saldırılarına karşı önceden gerekli hazırlıkları yapmamıza yardımcı olacağına inandığımız sonuçları sizlerle paylaşıyoruz.

YÖNETİCİ ÖZETİ

Uluslararası alanda devletlerin ve devlet dışı aktörlerin maruz kaldığı siber tehditler her geçen gün daha da çeşitlenmekte ve saldırılar şiddetlenmektedir. Söz konusu siber tehditlerin en önemlilerinden biri de hedefli fidye saldırılarıdır. Bu saldırı türünde tehdit aktörleri, hedef sisteme sızma gerçekleştirmek suretiyle çoğunlukla içerden kritik veri çalmakta ve sonrasında da verileri erişilemez hale getirmektedir. Bu durum siber güvenliğin üç kriteri olan olan gizlilik, erişilebilirlik ve bütünlük boyutlarını doğrudan etkilemektedir.

Küresel alanda faaliyet yürüten çok sayıda siber tehdit aktörünün son yıllarda araçlarını ve hedeflerini çoğalttığı görülmüştür. Buna bağlı olarak dünya çapında olağanüstü artış eğiliminde olan hedefli fidye saldırıları, pek çok devletin ve devlet dışı aktörün güvenlik politikalarını / stratejilerini şekillendirmektedir. Bu kapsamda özellikle gelişmiş devletler son iki yıl içerisinde siber güvenlik politikalarını güncellemiş ve ulusal siber altyapılarının güvenliğini sağlama adına kritik adımlar atmıştır.

Devletlere yönelik olarak gerçekleştirilen hedefli fidye saldırılarına ilaveten spesifik olarak hedef alınan sektörler de söz konusudur. Bu sektörler genellikle devletin ve kamunun yararı için çalışan ve birden çok sektörle doğrudan bağı bulunan kritik organlardır. Bahsi geçen sektörlerdeki şirketlerin ve devlet kurumlarının hedefli fidye saldırısına uğraması sonucunda, şirketler itibar ve para kaybına uğrarken, kamu kurumlarında ise tedarik sıkıntıları, iş süreç ve akışlarında aksamalar gibi bir çok problem meydana gelmektedir.

İşbu rapor 2021 yılında yaşanmış olan hedefli fidye saldırılarını, doğrudan saldırıyı gerçekleştiren tehdit aktörlerinin kendi platformlarında yayınlamış oldukları ilanlardan incelemek suretiyle hazırlanmıştır. TOR ağında yer alan 50 farklı tehdit aktörüne ait site/blog tespit edilerek, günümüzde çevrimiçi olan 27 tanesinin, 2021 yılında gerçekleştirildiği ve doğrudan üstlendiği 1239 adet saldırı incelenmiştir.

Çalışma kapsamında, son bir yılda küresel alanda gerçekleşmiş hedefli fidye saldırıları ülke, bölge ve uluslararası boyutuyla değerlendirilmiş ve hedef alınan sektörler / kurumlar tespit edilerek detaylı içerik analizi sunulmuştur. Gerçekleştirilen analizler neticesinde;

- 2021 yılında en çok hedefli fidye saldırısının, Amerika Birleşik Devletleri'nde ve Kanada'da yaşandığı,
- Avrupa kıtası, hedefli fidye saldırılarının dünya da en yoğun yaşandığı ikinci bölge olduğu ve en çok Birleşik Krallık, Almanya ve Fransa'nın hedef alındığı,
- Asya kıtasının ise en çok saldırının yaşandığı üçüncü bölge olup, burada sırasıyla Hindistan, Çin ve Japonya en çok hedefli fidye saldırısının yaşandığı ülkeler olduğu,
- Tüm dünyada sırasıyla en çok üretim, hizmet ve teknoloji sektöründe faaliyet yürüten şirketlerin hedef alındığı,
- En aktif hedefli fidye gruplarının Conti, Lock Bit ve Cl0p olduğu,

- Türkiye’de 2021 yılında yaşanan saldırıların hizmet, gıda, lojistik gibi bir çok sektöre dağıldığı,

- Türkiye’deki hedefli fidye saldırılarının XingTeam, Lock Bit ve AvosLocker tarafından gerçekleştirildiği,

tespit edilmiştir.

İlgili analizlere bağlı olarak gerçekleştirilen çatışan hipotezler analizine göre Türkiye’de 2022 yılında hizmet, üretim, teknoloji, sağlık, inşaat ve enerji sektörünün hedefli fidye grupları tarafından hedef alınması beklenmektedir.

GİRİŞ

Devletlerin, küçük / orta / büyük ölçekli şirketlerin, Sivil Toplum Kuruluşlarının ve bireysel kullanıcıların sıklıkla maruz kaldığı hedefli fidye saldırıları neredeyse her yıl en büyük siber tehditler listesinde ilk sıralarda yer almaktadır. Dünya çapında milyarlarca dolar zararlara neden olan saldırıların niteliği ve etkileri, tehdit aktörlerinin de çoğalmasıyla daha da artış göstermektedir.

Hedefli fidye saldırılarını yürüten tehdit aktörleri, kimi zaman devlet destekli gruplar, kimi zaman organize siber suç çeteleri, kimi zaman ise bireysel hackerlar olarak karşımıza çıkmaktadır. Temel amaçlarının hedefli fidye talep etmek olduğu düşünüldüğünde, bu tehdit aktörlerinin finansal motivasyonla hareket ettiği çıkarımı yapılabilmektedir. Ancak son zamanlarda yapılan hedefli fidye operasyonlarının birçoğunun finansal motivasyondan ziyade istihbarat toplama mahiyeti barındırdığı da değerlendirilmektedir.

Uluslararası alanda hedefli fidye saldırılarının neden olduğu büyük ölçekli zararların son bir yıl içerisinde ciddi oranda arttığı görülmektedir. Örneğin çeşitli devlet kurumlarının ve siber güvenlik şirketlerinin raporlarına göre 2020 yılındaki küresel hedefli fidye saldırıları, bir önceki yıla göre yüzde 150 artış göstermiştir Ayrıca saldırıya uğrayan kurbanların yaptıkları fidye ödemelerinde de yüzde 300'lere varan artışların olduğu tespit edilmiştir.

Kritik altyapılara, şirketlere ve kamu kurumlarına yapılan küresel hedefli fidye saldırıları 2021'in ilk çeyreğinde de olağanüstü bir artış göstermiştir. Saldırıların yoğunlaşmasıyla birlikte saldırganların kurbanlardan talep ettikleri fidye miktarlarında da dolaylı olarak büyük artışlar yaşanmıştır. Özellikle Bitcoin başta olmak üzere pek çok kripto para varlıklarının değerinin yükselmesinden dolayı dünya çapında hizmet yürüten şirketlerin saldırganlara ödedikleri fidyelerin toplamı milyar dolarlar seviyesindedir.

Bu çalışmada, son bir yılda küresel alanda gerçekleşmiş hedefli fidye saldırıları ülke, bölge ve uluslararası boyutuyla değerlendirilmiş ve hedef alınan sektörler / kurumlar tespit edilerek detaylı içerik analizi sunulmuştur. Çalışmanın amacı, 2021 yılında hedefli fidye saldırısı gerçekleştirmiş olan grupların son bir yılı incelenmek suretiyle, 2022 yılında hedef alınması muhtemel sektörlere yönelik bir ön değerlendirme sunmaktır.

Çalışma kapsamında kullanılmış olan veri seti;
TOR ağında bulunan 50 farklı fidye grubuna ait çeşitli çevrimiçi platformların tespit edilmesi suretiyle, doğrudan birincil kaynaklardan elde edilmiştir. Veri seti; grupların bizzat kendileri tarafından kullanılan ve erişilebilir durumda olan 27 kanaldaki 2021 yılına ait toplam 1239 adet saldırının;

Saldırıyı gerçekleştiren grup,
- Saldırı tarihi,
- Hedef alınan kuruluş,
- Hedef kurluşa ait ülke ve kıta bilgisi,
- Veri ihlal durumu,

bilgilerinden oluşmaktadır.

Öte yandan bazı saldırı gruplarının eylemi gerçekleştirmiş oldukları tarihi belirtmemeleri sebebiyle ilgili bölümün bazı satırlarında eksiklikler bulunmaktadır. Ayrıca veri setinin hazırlandığı esnada Rusya menşeli olduğu iddia edilen REvil fidye grubunun Rus kolluk kuvvetleri tarafından kapatılmış olması sebebiyle ilgili grubun eylemlerine doğrudan ulaşılamamıştır.

Çalışmanın ilk bölümünde günümüzde yaşanan hedefli fidye saldırılarına genel bir bakış sunulmuştur. Bölüm kapsamında; öncelikle küresel alanda yaşanan hedefli fidye saldırılarının durumu, saldırıların yol açtığı kaos ve oluşturduğu algı çerçevesinde değerlendirmeler yapılmıştır. Böylece okuyucunun hedefli fidye saldırıları hakkında genel bilgiye sahip olup, dünyada bu tür saldırıların etkileri ve çerçevesi hakkında da fikir edinmesi hedeflenmiştir.

Çalışmanın ikinci bölümünde 2021 yılında gerçekleştirilen küresel hedefli fidye operasyonlarındaki trend incelenmiştir. İncelemede tarafımızca hazırlanmış ve doğrudan birincil kaynaklardan alınan veriler sayısal yöntemlerle analiz edilmiş, böylece 2021 yılında hangi sektörlerin, hangi aktörler tarafından hedef alındığı gibi eğilimlerin tespit edilmesi amaçlanmıştır.

Çalışmanın üçüncü kısmında ise Türkiye'de faaliyet göstermekte olan şirketleri hedef almış tehdit aktörleri özelinde inceleme gerçekleştirilmiştir. Bu inceleme kapsamında tehdit aktörlerinin Türkiye ve globaldeki kesişen eylemleri bütüncül olarak incelenmiştir. İnceleme sonucunda hedefli fidye gruplarının saldırılarına dair asgari teknik bilgiye sahip bir okuyucunun anlayacağı düzeyde teknik açıklamalara yer verilmiştir. Böylece devlet kurumlarında ve özel sektördeki ilgili birimlerin Türkiye'ye odaklanmış ve odaklanması muhtemel tehdit aktörlerine yönelik bir ön değerlendirme yapabilmesi mümkün olabilecektir.

Çalışmanın sonuç kısmında ise Türkiye'de potansiyel olarak hedef alınabilecek sektörlere yönelik bir değerlendirme sunulurken, olası tehditleri asgari düzeye indirme amacıyla kurumların alabilecekleri önlemler özelinde genel tavsiyelerde bulunulmuştur.

1 - HEDEFLİ FİDYE SALDIRILARINA GENEL BAKIŞ

Hedefli fidye saldırıları, dünya çapında çok önemli bir güvenlik sorunu olarak görülmektedir. Siber tehdit aktörleri, hedef aldıkları bilgisayar sistemlerine yönelik siber müdahaleler sonucu verileri kendi sunucularına aktardıktan sonra silmekte ve / veya şifreleyip erişilemez duruma getirmektedir. Verilerin geri yüklenmesi, çözülmesi ve / veya ifşa edilmemesi karşılığında fidye talep edilen bu siber suç türü, oldukça ciddi maddi zararlara yol açmaktadır.

Yıllardır dünyayı tehdit eden hedefli fidye operasyonlarının aktörleri de saldırılarla paralel olarak artmaktadır. Profesyonel anlamda teknik bilgi, donanım ve kapasiteye sahip olan aktörler, aynı yetenek ve kapasiteye sahip olmayan diğer tehdit aktörlerine, "Ransomware as a Service" (RaaS) olarak da adlandırılan hizmet ya da iş birliği çerçevesinde faaliyetlerini pazarlayarak teknik bilgi ve kapasitesi yetersiz aktörlerin de siber uzayda hedefli fidye saldırısı gerçekleştirmelerine imkan sunmaktadır. Bu durum tehdidin daha da artmasına ve etkisinin genişlemesine yol açmaktadır.

Hedefli fidye saldırılarını yürüten siber tehdit aktörleri, kimi zaman devlet destekli gruplar, kimi zaman organize siber suç çeteleri, kimi zaman ise bireysel hackerlar olarak karşımıza çıkmaktadır. Temel amaçlarının fidye talep etmek olduğu düşünüldüğünde, bu tehdit aktörlerinin finansal motivasyonla hareket ettiği çıkarımı yapılabilir.

Buna ek olarak son zamanlarda yapılan hedefli fidye operasyonlarının birçoğunun finansal motivasyondan ziyade istihbarat toplama ve sabotaj amacını taşıdığı görülmektedir. Verilerin, hedef kurum sisteminde şifrelenmeden ve / veya silinmeden önce saldırganın kontrolündeki komuta kontrol (C2) sunucusuna yedekleniyor olması, eylemin espiyonaj maksadı barındırdığı yönündeki değerlendirmenin artmasına neden olmaktadır. Öte yandan fidye maskesi altında esas hedefinin "yok etme, hasar verme" olduğu belirlenen "wiper" türündeki zararlı yazılımların da kullanıldığı görülmektedir.

Geçmişten günümüze kadar hedefli fidye saldırılarının neden oluğu güvenlik sorunları hem devletler hem de şirketler boyutunda önem arz etmektedir. Şirketlere, kamu kurumlarına, ulusal kritik altyapılara ve sivil kuruluşlara yönelik hedefli fidye saldırılarına küresel boyutta bakıldığında "uluslararası güvenliğe ciddi bir tehdit" söz konusudur.

2017 yılında dünyada on milyarlarca dolar zararlara neden olan ve hem devletlerin hem de dev şirketlerin adeta kabusu haline gelen WannaCry ve NotPetya saldırılarından sonra tehdit aktörleri ve varyantlar sürekli olarak artış göstermiştir. Çoğunlukla Rusya, Çin ve Kuzey Kore menşeli olduğu iddia edilen bu aktörlerin bazıları devlet destekli gruplar bazıları ise organize finansal motivasyonlu oluşumlar olarak karşımıza çıkmaktadır.

Sayısal veriler ışığında, hedefli fidye operasyonlarının geldiği nokta endişe vericidir. Uluslararası alanda hedefli fidye saldırılarının neden olduğu büyük ölçekli zararların son bir yıl içerisinde ciddi oranda arttığı görülmektedir. Örneğin 2020 yılındaki küresel hedefli fidye saldırılarının, bir önceki yıla göre yüzde 150 artış gösterdiği; ayrıca saldırıya uğrayan kurbanların yaptıkları fidye ödemelerinde de yüzde 300'lere varan artışların olduğu tespit edilmiştir.[1]

[1] The 2021 Crypto Crime Report, "Chainalysis", February 2021. (Erişim Tarihi: 12.02.2022)

Kurbanların tehdit aktörlerine yönelik fidye ödemelerinde görülen artışlar, söz konusu aktörlerin "iştahını kabartan" unsurlardandır. Kripto paraların yaygınlaşması, çeşitlenmesi ve değerinin artmasıyla birlikte saldırılardan mağdur olan kurbanların yaptığı ödemeler tehdit aktörlerinin eylemlerinin artması yönünde bir önemli etkiye sahiptir.

Günümüze gelindiğinde hedefli fidye operasyonlarının özellikle ABD'de ve birçok AB ülkesinde yükselişe geçtiği gözlemlenmektedir. 2021 yılının ilk ve ikinci çeyreğinde hedefli fidye saldırılarına dair çok sayıda vaka bildirilmiştir. ABD'de hayatı adeta durma noktasına getiren Colonial Pipeline saldırısı ve ülkenin en büyük sigorta şirketlerinden olan CNA Financial'a yönelik saldırılardan kısa bir süre sonra Avrupa'da da büyük şirketler hedefli fidye saldırılarının kurbanı olmuşlardır.

ABD'deki bu tarz saldırıların artışa geçtiği o dönemde Rus REvil, DarkSide ve Evil Corp gibi organize gruplar hedefli fidye saldırılarını gerçekleştiren aktörler olarak açıklanmıştır. Söz konusu saldırılar sonrasında şirketlerin toplamda 50 milyon dolara yakın fidye ödemesi yaptığı da iddialar arasında yer almaktadır.

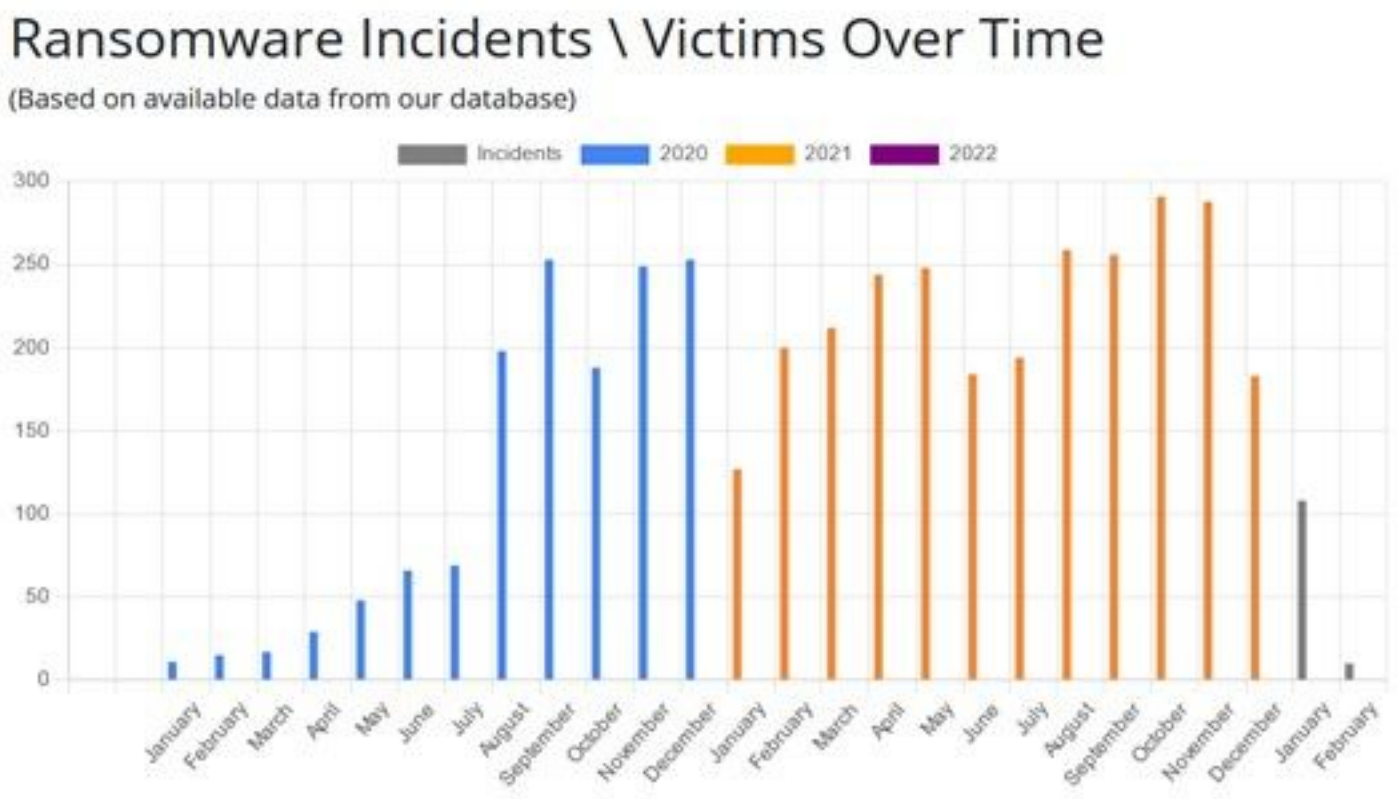
Küresel boyuta gelindiğinde ise sayısal veriler ışığında finansal kayıpların çok daha fazla olduğu net bir şekilde görülmektedir. Örneğin, küresel fidye saldırıları sonrası yapılan fidye ödemeleri 2020 yılında 400 milyon doları aşmış, 2021'in ilk 6 ayında ise 590 milyon dolarlık fidye ödemeleri yapılmıştır.[2]

Diğer yandan 2020 ve 2021 arası dönemde İran-İsrail cephesinde de hedefli fidye operasyonlarının sürdüğü gözlemlenmiştir. İsrail tarafından doğrudan İran devleti ile ilişkilendirilen Pay2Key grubu ve Black Shadow grupları, çok sayıda İsrailli şirkete yönelik saldırılar gerçekleştirmiştir.

[2]U.S. Department of the Treasury, "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange" https://home.treasury.gov/news/press-releases/jy0471, (Erişim Tarihi: 14.02.2022)

2 - 2021'de HEDEFLİ FİDYE SALDIRILARI TRENDİ

Hedefli fidye saldırıları küresel olarak hızlı bir artış seyrindedir. Geçmiş yıllara oranla 2021 yılını değerlendirdiğimizde birçok farklı kaynak bu iddiayı doğrulamaktadır. Ransom-DB tarafından yayınlanmış aşağıdaki grafik söz konusu artışa yönelik örnek olarak gösterilebilir[3]. Bu artışa yönelik birçok somut bulgu, farklı kurum ve kuruluşlar tarafından yayınlanmış olan raporlarda da gözlemlenmektedir.



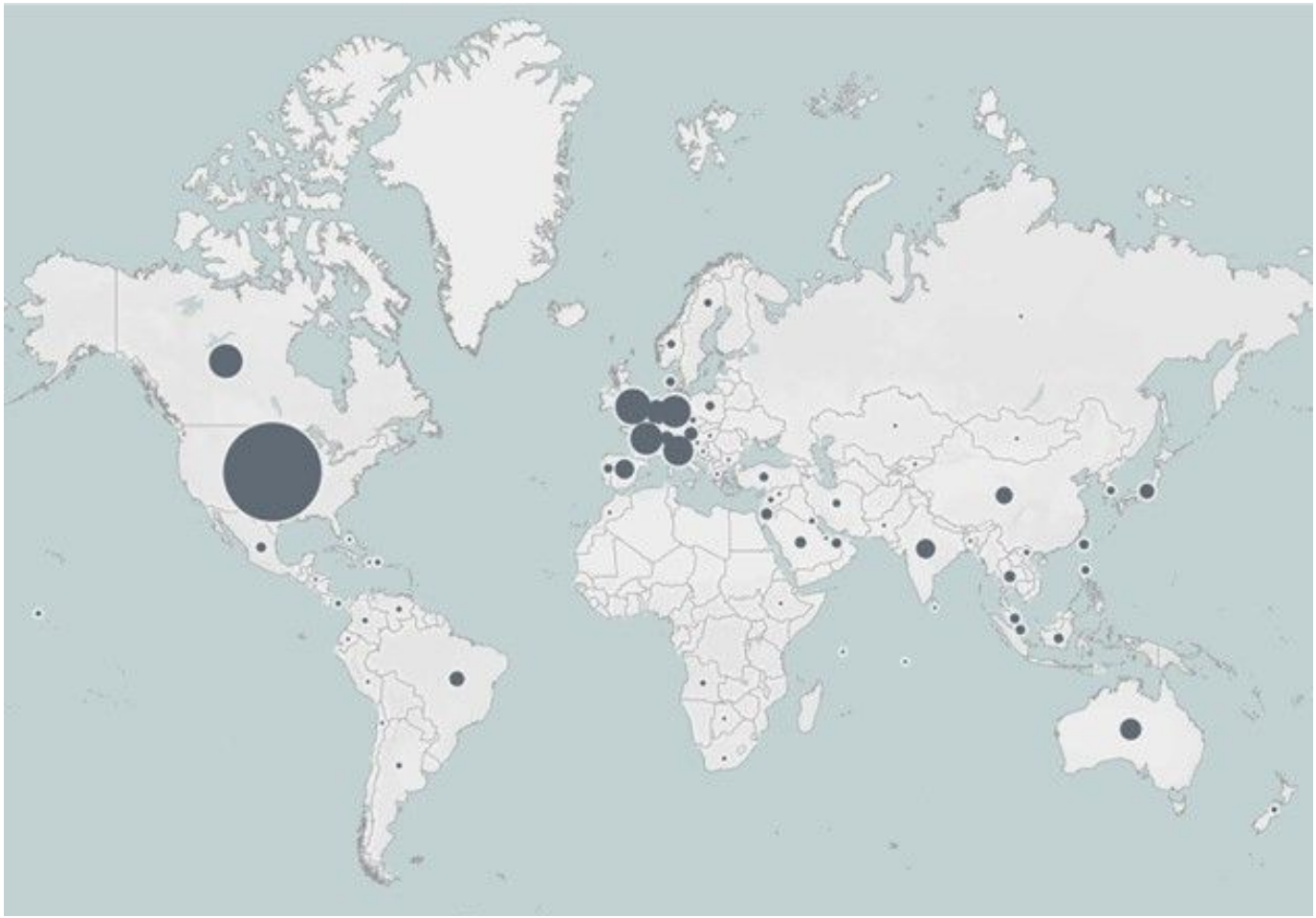
Grafik 1: Ransom-Db tarafından yayınlanan istatistik

2021 yılında gerçekleşmiş olan hedefli fidye saldırılarına doğrudan birincil kaynaklardan elde edilen veriler çerçevesinde baktığımızda ise 1239 saldırının tehdit aktörlerince duyurulduğu görülmektedir. Öte yandan bahse konu 1239 saldırı, gerçekleştirmiş olduğumuz OSINT çalışması neticesinde varlığını doğruladığımız 50 farklı tehdit aktörünün 27'sine ait olan TOR ağındaki platformlarında tespit edilen saldırılardır. Verilerin toplandığı esnada platformu kapalı olan ya da kolluk kuvvetleri tarafından faaliyetine son verilen diğer 23 tehdit aktörüne yönelik veriler, bu saldırı listesine dahil değildir. Ayrıca bazı hedefli fidye grupları, fidyenin ödenmesi durumunda hedef şirkete ait bildiriyi kaldırmaktadır. Dolayısıyla 2021 yılında gerçekleşen saldırıların 1239'dan çok daha fazla olduğunun altını çizmek gerekir.

[3] Ransom-DB, https://www.ransom-db.com/ransomware-statistics , (Erişim Tarihi: 04.02.2022)

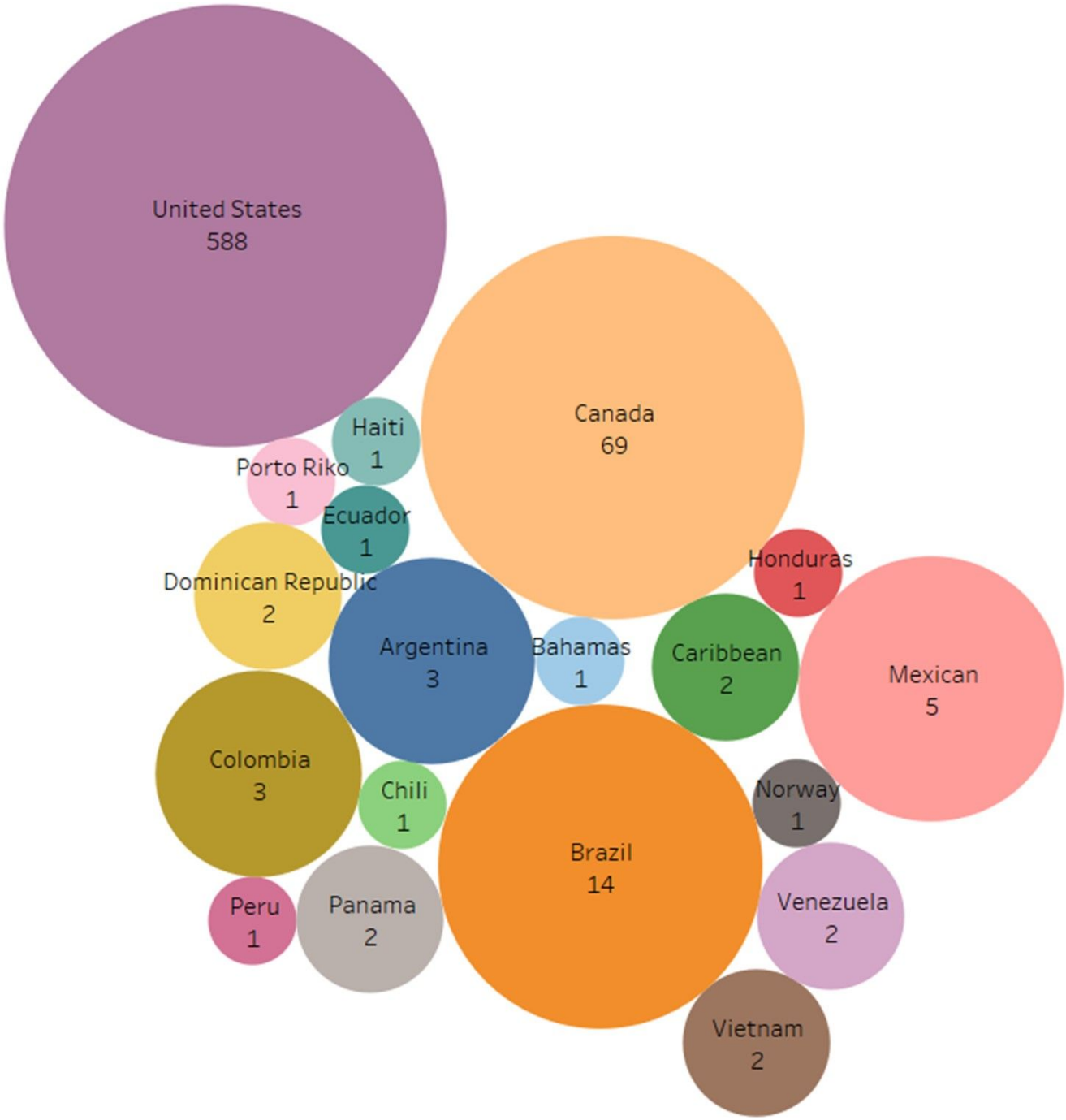
Bahsi geçen 1239 saldırının doğrudan tehdit aktörleri tarafından üstlenilen eylem olduğu ve bunların birçoğuna ait bilginin kamuya duyurulmadığı göz önünde bulundurulduğunda, 2021 yılında gerçekleşmiş olan saldırılara yönelik gerçekçi bir bilanço ortaya koymak mümkündür.

Bu bağlamda ilgili verileri değerlendirdiğimizde ilk olarak karşımıza çıkan bulgu, aşağıdaki haritada yer verildiği gibi, dünyada en çok hedefli fidye saldırısının yaşandığı kıtaların dağılımıdır.



Grafik 2: 2021 yılında yaşanan hedefli fidye saldırılarının kıta bazlı yoğunluğu

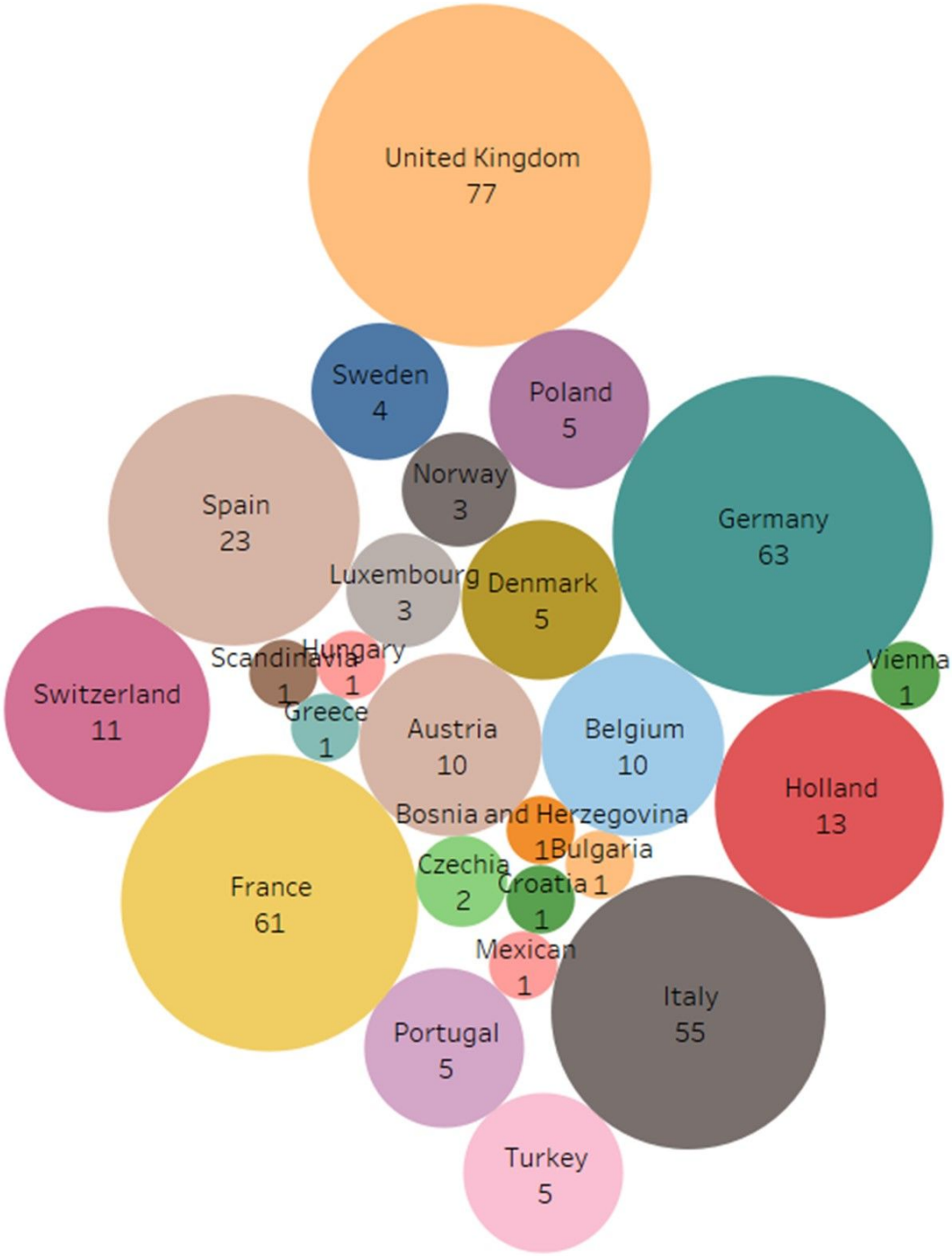
Haritada da görüldüğü üzere 2021 yılında en fazla hedefli fidye saldırısının yaşandığı ülke Amerika Birleşik Devletleri'dir. Hedefli fidye grupları 2021 yılında sadece ABD'de 588 şirketi hedef aldıklarını açıklamışlardır. Kıta bazında baktığımızda ise bu bölge yine en çok saldırının gerçekleştiği bölge olarak görülmekte ve toplamda 700 saldırının gerçekleştiği gözlemlenmektedir. Buna ek olarak Kanada'da 2021 yılı içerisinde 69 saldırının gerçekleştirildiği de verilerimiz arasında yer almaktadır. Bütüncül olarak baktığımızda tüm Amerika kıtasında hedef seçilen ülkelerin dağılımında ise karşımıza sırasıyla ABD, Kanada ve Brezilya çıkmaktadır.



Grafik 3: Amerika kıtasında yaşanan hedefli fidye saldırılarının ülkelere göre dağılımı

Hedefli fidye operasyonlarında çoğunlukla Amerika Birleşik Devletleri'nin hedef alınması noktasında jeopolitik açıdan bazı yorumlar yapılabilir. Uzun zamandır Rus ve Çin menşeli hedefli fidye grupları tarafından hedef alınan bu ülkede zarar gören kurbanların kritik devlet kurumları ve büyük ölçekli şirketler olduğu dikkat çekmektedir. Aynı şekilde su tesisleri, petrol istasyonları gibi sivil kritik altyapıların da hedefler arasında olduğu görülmektedir. 2020 yılından itibaren özellikle Rus menşeli REvil, DarkSide gibi siber tehdit aktörlerinin adı geçen hedeflere yönelik hedefli fidye operasyonları söz konusudur. Kremlin destekli olduğu iddia edilen ve NSA, Pentagon gibi önemli kurumlara yapılan saldırıların fidye araçlarıyla yapıldığı görülse de bu operasyonlarda esas maksadın siber casusluk olabileceği öne sürülebilir.

Dünyada en çok saldırının gözlemlendiği ikinci ülke ise 77 saldırı ile Birleşik Krallık'tır. Ayrıca Avrupa kıtası Grafik 2'de de görüldüğü üzere dünyada en fazla saldırının gözlemlendiği ikinci bölgedir. Bu kıta özelinde saldırılara baktığımızda ise Avrupa'nın başat aktörlerinin öncelikle hedef alındığı dikkat çekmektedir. Grafikte de görüldüğü üzere Birleşik Krallık, Almanya ve Fransa sırasıyla Avrupa kıtasında hedefli fidye grupları tarafından en çok hedef alınan ülkelerdir.



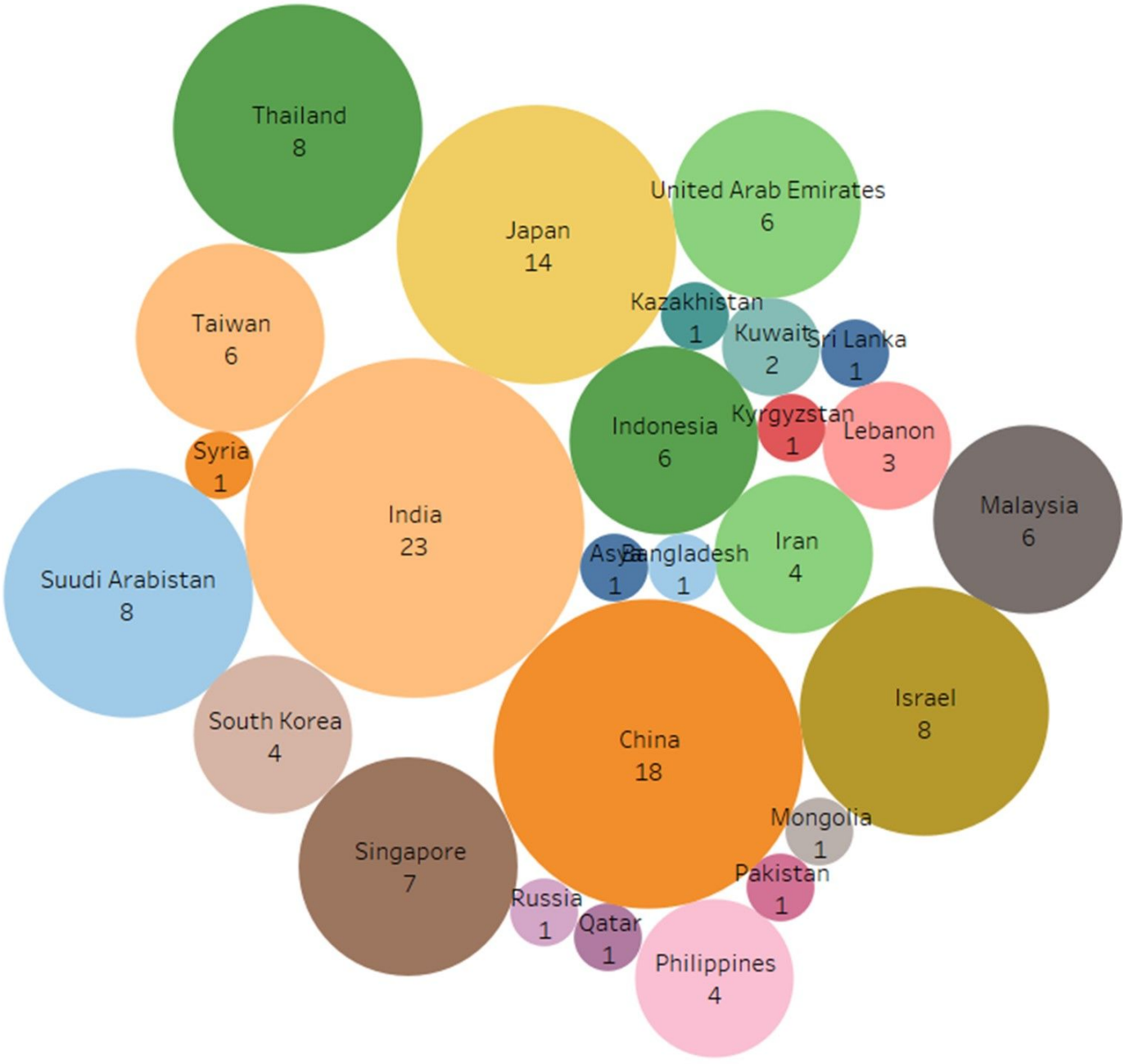
Grafik 4: Avrupa kıtasında yaşanan hedefli fidye saldırılarının ülkelere göre dağılımı

Avrupa'daki en çok hedef alınan ülkeleri listeden ayrı tuttuğumuzda, Türkiye ortalama düzeyde hedef alınan ülke konumundadır. Bu durum, fidye ödemeleri sonrasında, birçok tehdit aktörünün veri tabanından saldırıya dair duyuruları kaldırmasından kaynaklanmaktadır. Dolayısıyla Türkiye'ye yönelik saldırıların Almanya ya da Fransa kadar sık olmasa da en az İspanya kadar olabileceğini söylemek mümkündür.

Ayrıca Türkiye'deki şirketlerin gelir durumu, fidye sigortaları ve ödeme eğilimleri Avrupa'nın diğer gelişmiş ülkelerine oranla daha düşüktür. Sonuç olarak tehdit aktörlerinin İngiltere'yi öncelikli seviyede hedef alırken, Türkiye'yi bir geçiş sahası olarak kullandığı yorumu da yapılabilir.

Fakat Türkiye'deki saldırılara baktığımızda, geleneksel bir hedefli fidye saldırısından ziyade hedef odaklı bir saldırının olduğu gözlemlenmekte ve saldırganların "stratejik niyetlerle" Türkiye'de yer alan bazı kuruluşlara saldırdığı görülmektedir. Türkiye'deki şirketlerin hızlı gelişimi ve uluslararası pazarlardaki payının katlanarak arttığı, buna bağlı olarak da yıllara oranla 2021'de yaşanan Türkiye'deki hedefli fidye saldırılarını birlikte yorumladığımızda, gelecekte birçok kurum ve şirketin önemli oranda hedef alınacağı söylenebilir.

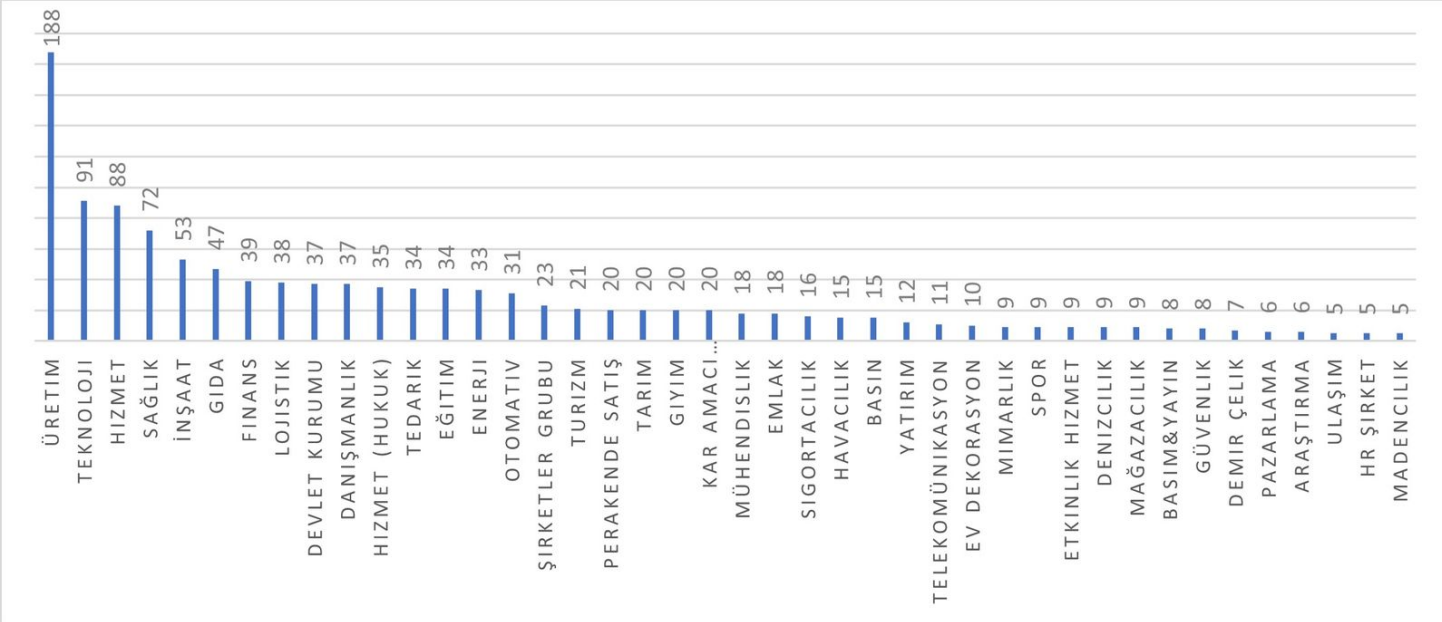
Küresel hedefli fidye operasyonlarını incelerken Asya kıtasına baktığımızda ise 2021 yılında 23 saldırı ile Hindistan'ın bölgedeki birincil hedef olduğu gözlemlenmektedir. Bölgede en çok hedef alınan diğer ülkeler ise 18 saldırı ile Çin ve 14 saldırı ile Japonya'dır.



Grafik 5: Asya kıtasında yaşanan hedefli fidye saldırılarının ülkelere göre dağılımı

Toplamış olduğumuz veriler ışığında 2021 yılında yaşanan hedefli fidye saldırılarına sektörel bazda baktığımızda ise aşağıdaki grafikte de görüldüğü gibi en çok 188 saldırı ile üretim sektörünün hedef alındığı görülmektedir. Bu üretim sektörü içerisinde inşaat sektörü için çelik konstrüksiyon üretimi yapan firmalardan, sağlık sektörü için enjeksiyon, teknoloji şirketleri için kablo üretimi gerçekleştiren şirketlere kadar birçok farklı kuruluş bulunmaktadır.

Üretim sektöründen sonra en çok saldırı alan bir diğer sektör ise hizmet sektörüdür. Grafiğe göre 2021 yılında en çok saldırı alan sektör teknoloji görünse de hizmet sektörüne dahil edilebilecek danışmanlık, hukuk, finans gibi farklı alanlarda faaliyet yürüten şirketleri genel olarak topladığımızda, teknoloji sektöründen çok daha fazla saldırının yaşandığını söylemek mümkündür. Bu anlamda bütün hizmet sektörü, 165 saldırı ile üretim sektöründen sonra en çok saldırının gerçekleştiği ikinci sektördür.



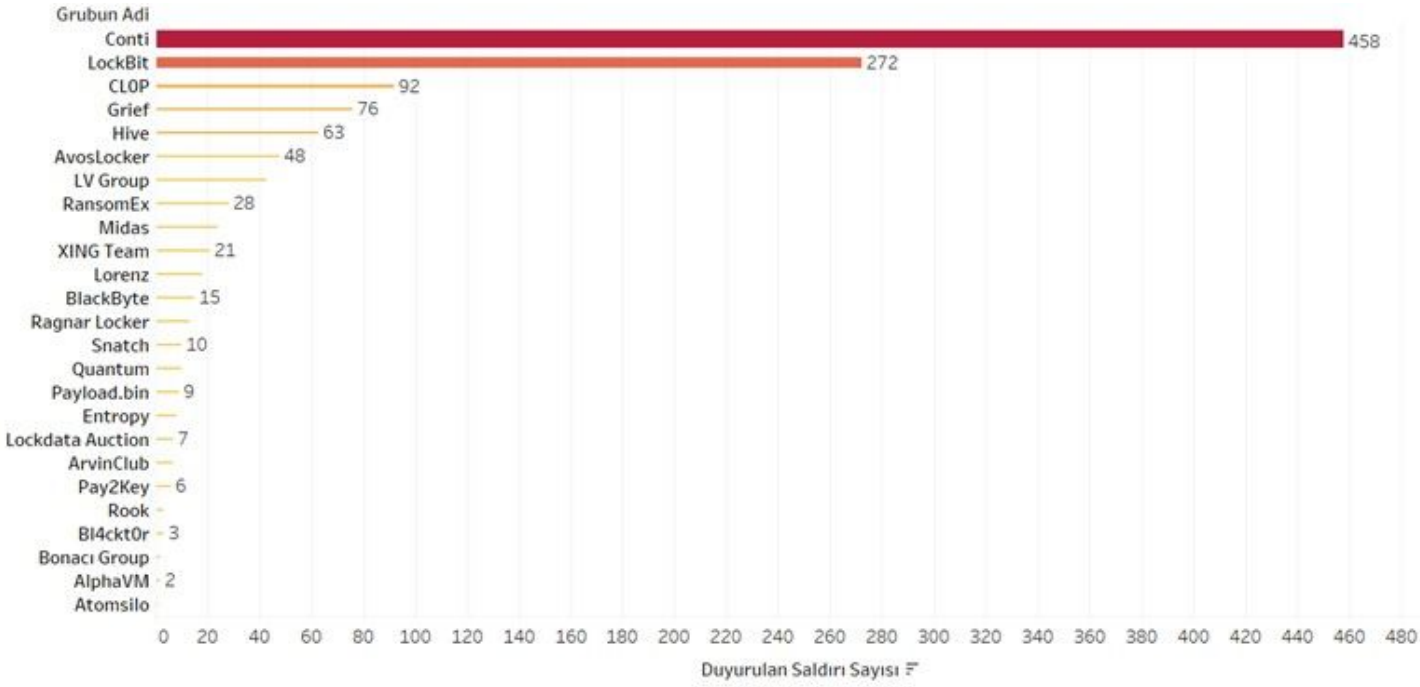
Grafik 6: 2021 yılında hedef alınan sektörler

Bu üç sektör özelinde bir değerlendirme yaptığımızda hem şirketlerin kar marjının diğer bir çok şirketten daha yüksek olması, hem de bu şirketlerde işleyişin durması halinde oluşabilecek zararın diğer sektörlerde faaliyet yürüten şirketlere göre daha fazla olduğu görülmektedir. Öte yandan bu sektörde yer alan şirketler, diğer birçok sektör için "ana kaynağı" oluşturmaktadır. Haliyle bu sektörlerde meydana gelen aksama diğer sektörlerdeki işleyişi de etkilemektedir. Dolayısıyla stratejik açıdan bakıldığında, bu sektörlerin öncelikli olarak hedeflenmesi ihtimali göz ardı edilmemelidir.

2021 yılında en çok saldırı gerçekleştirdiğini duyuran hedefli fidye gruplarına baktığımızda ise ilk sırada geçtiğimiz yıllarda da adı listelerin başında yer alan Conti grubu karşımıza çıkmaktadır. Conti'yi her zaman olduğu gibi Lock Bit ve Cl0p takip ederken, Grief ve Hive de 2021'in en aktif hedefli fidye grupları arasındadır. REvil'in aşağıdaki grafikte ve listede yer almamasının sebebi ise daha önce belirtildiği gibi listenin hazırlandığı esnada Rus istihbarat servisi FSB ve diğer kolluk kuvvetleri tarafından faaliyetlerine son verilmesidir. Fakat REvil'in uzun yıllardır sürdürmüş olduğu aktif faaliyetleri düşünüldüğünde, şu an için faaliyetlerinin sürüp sürmeyeceği belirsiz olsa dahi son derece yetenekli ve spesifik araçlara sahip bir tehdit aktörü olduğunu belirtmek gerekir.

ABD için son yılların en büyük siber tehdit unsuru olarak kabul edilen REvil grubu, finansal motivasyonlu olarak hareket etse de hedef aldığı ülkeler ve sektörlere bakıldığında ideolojik veya politik bir boyuttan da bahsetmek mümkündür. Nitekim REvil grubunun hedef almadığı ülkelerin Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) döneminden sonra oluşan Bağımsız Devletler Topluluğu üyesi ülkeler olduğu bilinmektedir. Ayrıca Batılı kaynakların belirttiğine göre REvil grubunun operasyonlarda kullandığı hedefli fidye araçlarının adı geçen devletlerde pasif hale geçtiği görülmektedir. Dolayısıyla REvil grubunun Kremlin'in dış politikası doğrultusunda, jeopolitik çıkarları da gözeterek hareket ettiği öne sürülebilir.

RansomDB tarafından oluşturulan bir istatistiğe göre REvil grubu 286 saldırı ile en aktif üçüncü grup olarak görülmektedir. Fakat RansomDB tarafından hazırlanan listede tamamen faaliyetleri sonlanmış grupların da bulunuyor olması ve tarih aralığının belirtilmemesi sebebiyle 2021 yılı için REvil'i bir sıralamaya almak mümkün görünmemektedir.

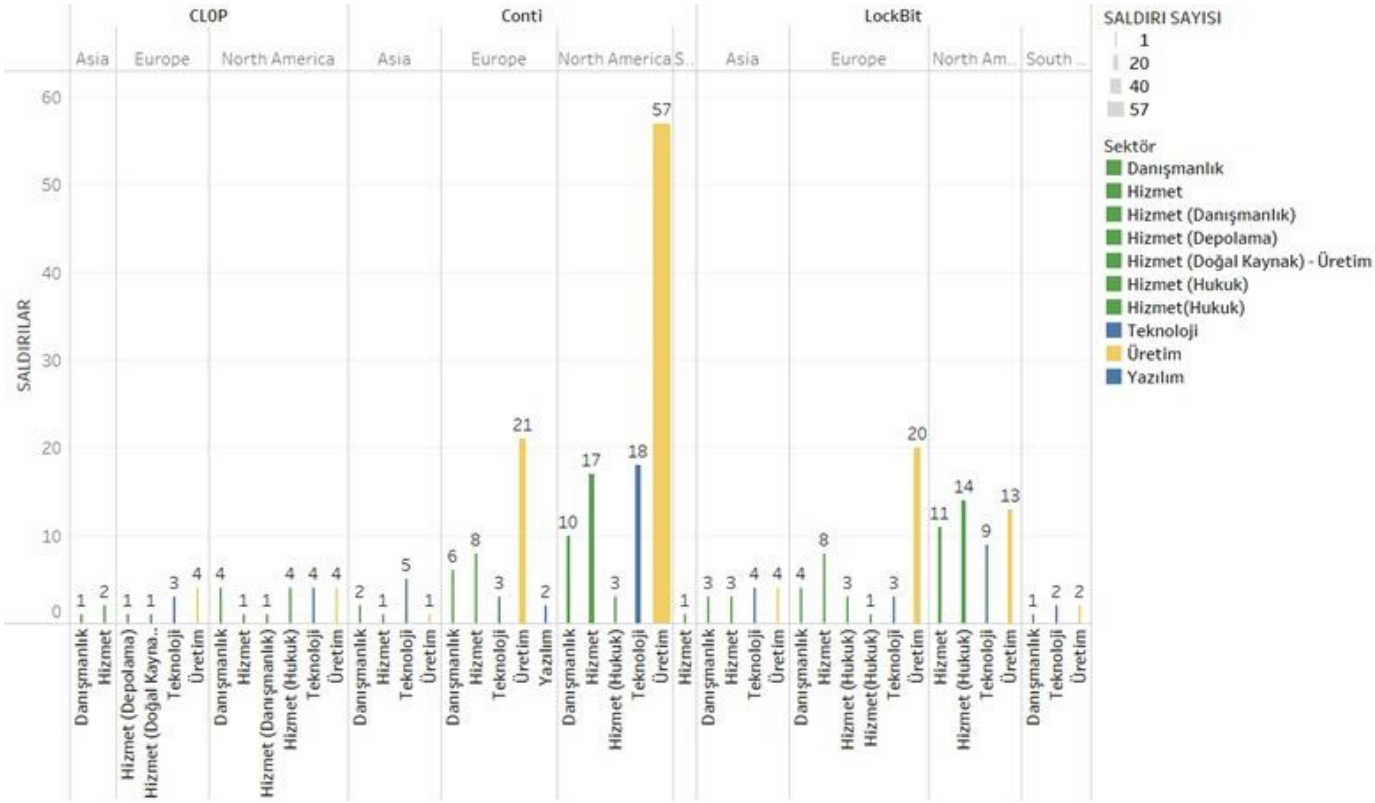


Grafik 7: 2021 yılında en çok hedefli fidye saldırısı gerçekleştiren aktörler

Çalışmanın üst kısımlarında yer verilmiş olan, en sık saldırının göründüğü kıtalar, sektörler ve tehdit aktörleri özelinde bir değerlendirme yaptığımızda; Amerika kıtasında 105 operasyon gerçekleştiren Conti'nin, bu saldırılardan 30'unu hizmet sektörüne, 18'ini teknoloji sektörüne ve 57'sini üretim sektörüne gerçekleştirdiği görülmektedir. Saldırganların Avrupa kıtasındaki operasyonlarının ise aynı dizilim bağlamında neredeyse 3'te 1'e düştüğü ve bu kıtada daha çok üretim ve hizmet sektörlerini hedef aldığı görülmektedir. Asya kıtasında ise Conti grubu en çok teknoloji sektörünü hedef almıştır.

LockBit'in eylemlerine baktığımızda ise Amerika kıtasında 47 saldırı ile hizmet, teknoloji ve üretim sektörlerine en çok saldıran ikinci hedefli fidye grubu olduğu görülmektedir. Tehdit aktörleri Amerika kıtasında en çok 25 saldırı ile hizmet sektörünü hedef almıştır. Üretim sektörü özelinde grubun saldırılarına baktığımızda ise Amerika kıtasında 13 iken, Avrupa kıtasında 19 olduğu görülmektedir. Kısaca LockBit grubu, üretim sektörünü hedef aldığı eylemlerini daha çok Avrupa kıtasındaki ülkelere yönelik gerçekleştirmektedir. Grubun Asya'da ise teknoloji ve üretim sektörüne yönelik saldırıları eşit orandadır.

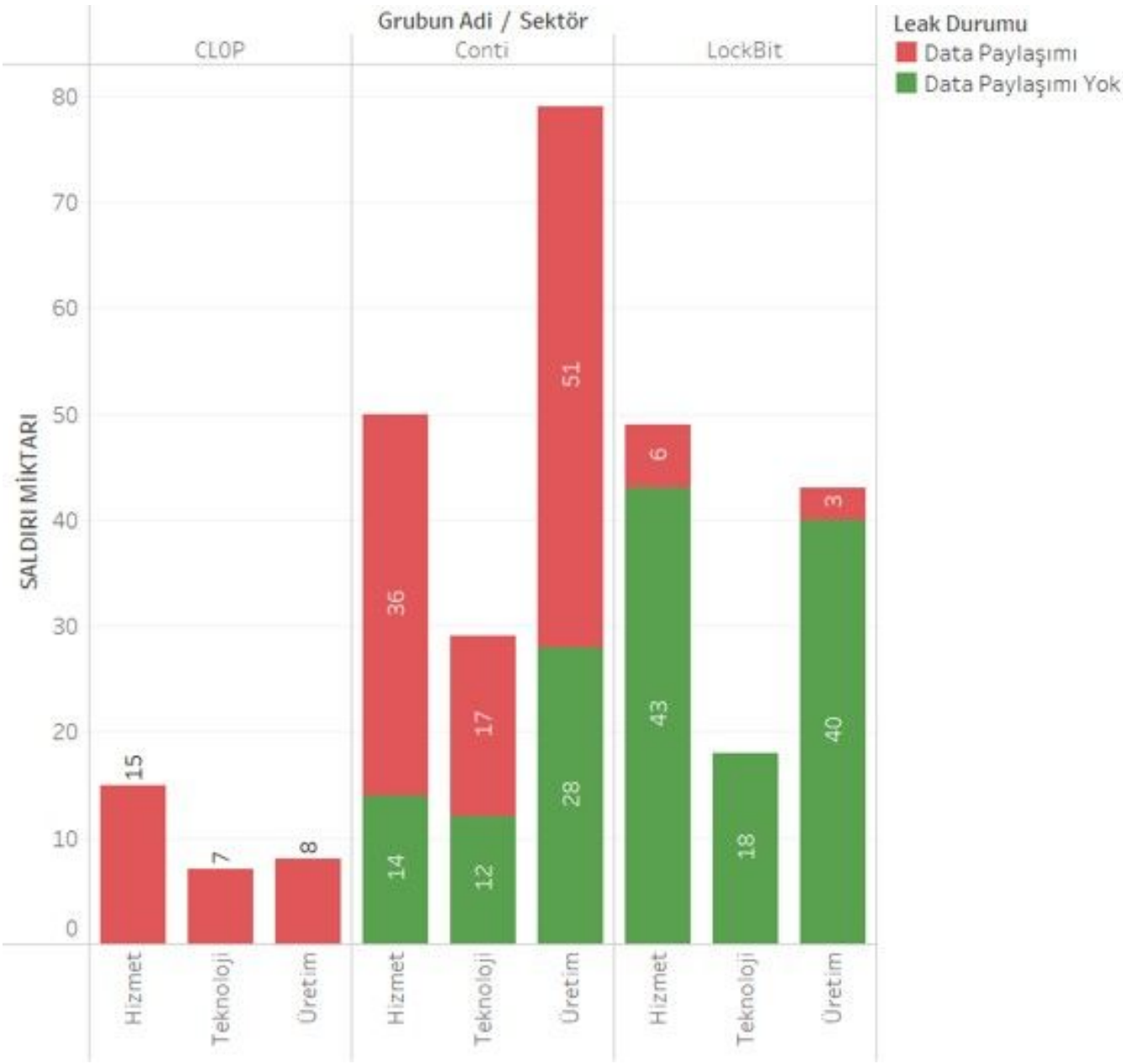
Cl0p'un eylemlerine baktığımızda ise Amerika'da diğer iki aktöre göre daha az eylem düzenlediği görülmektedir. Bu bağlamda grup, Amerika kıtasında hizmet sektörüne yönelik 10 saldırı gerçekleştirmişken, Avrupa kıtasında 2, Asya kıtasında ise 3 saldırı yapmıştır. Grubun verilerine yönelik dikkat çekici nokta ise Asya kıtasında sadece hizmet sektörünü hedef alırken, teknoloji ve üretim sektörüne yönelik herhangi bir saldırı yapmamasıdır.



Grafik 8: 2021 yılının en aktif hedefli fidye grupları ve en çok hedef olan sektörlere yönelik saldırılar

Son olarak tehdit aktörlerinin üç ana sektördeki eylemleri sonrasında ele geçirmiş oldukları verileri paylaşıma açıp açmadıklarına baktığımızda Conti'nin büyük oranda veri paylaşımı gerçekleştirdiği görülmektedir. LockBit ise bu sektörlerdeki eylemleri sonrasında ele geçirmiş olduğu verileri daha çok "tehdit aracı" şeklinde kullanmakta ve doğrudan paylaşmak yerine, verilerin satışını yapmaktadır. Cl0p ise her üç sektördeki eylemlerinde ele geçirmiş olduğu verileri paylaşmaktadır. Aşağıdaki tabloda bu üç tehdit aktörüne ait eylemler görülmektedir.

Grupların saldırılarda ele geçirdikleri verileri paylaşmalarındaki genel motivasyon, hedef şirketin fidye ödeme ihtimalini arttırmaktır. Birçok şirket için, müşterileri, çalışanları, finansal kayıtları, üretim ve iş akışlarına yönelik bilgiler, talep edilen fidye miktarından çok daha fazlasını ifade etmektedir. Bunun farkında olan tehdit aktörleri çoğunlukla saldırıyı kamuya duyurdukları esnada örnek veri paylaşımı da yapmakta ve fidyenin ödenmemesi durumunda kademeli olarak geri kalan verileri paylaşmaktadır.



Grafik 9: En aktif hedefli fidye gruplarının, en yaygın saldırı yaşanan sektörlere ait veri sızdırma miktarı

3 - TÜRKİYE'YE YÖNELİK HEDEFLİ FİDYE SALDIRILARI VE TEHDİT AKTÖRLERİNE DAİR DEĞERLENDİRME

Dünya genelinde 2021 yılında yaşanmış olan hedefli fidye saldırılarını analiz ettiğimiz veri setinde Türkiye için bir inceleme yaptığımızda, dünya trendleriyle paralel gelişmelerin yaşandığı görülmektedir. Sayısal açıdan Türkiye'de yaşanan olaylara baktığımızda saldırganlar tarafından doğrudan duyurulan 5 saldırıdan ikisinin LockBit, ikisinin XING Team ve diğerinin de AvosLocker tarafından gerçekleştirildiği gözlemlenmektedir.[4] Saldırıya uğrayan şirketlerin isimlerini gizli tutmak suretiyle aşağıda paylaşılmış olan grafikte hangi hedefli fidye grubunun, hangi sektörde faaliyet yürüten şirketi hedef aldığı, bu eylemi ne zaman duyurduğu, şirket merkezinin nerede bulunduğu ve saldırı sonrasında bir veri ihlalinin olup olmadığı görülmektedir.

Grafik 10: Türkiye'de yaşanan hedefli fidye saldırılarına ait bilgiler

Grafikte de görüldüğü üzere 2021 yılında Türkiye'de faaliyet yürüten şirketlere ilk hedefli fidye saldırısını gerçekleştirmiş olan grup Xing Team'dir. 2021 yılında eylemlerine başlayan grup, veri setinin hazırlandığı esnada Tor ağındaki kanallarının açık olmasına karşın Şubat ayı itibariyle sayfasını taşımış/kapatmıştır. Genel hatlarıyla Xing Team'e baktığımızda isminin Mandarincede "Star" anlamına gelen bir kelimeden geldiği görülmektedir.

[4]Bu saldırıların dışında Türkiye'de daha çok sayıda hedefli fidye saldırısının yaşandığı bilinmektedir. Fakat bu saldırıların çoğunun gizli / örtülü kaynaklarda yer alması ve verilerin, saldırıyı gerçekleştiren gruplar tarafından ilgili platformlardan kaldırılması sebebiyle Türkiye için bu 5 eylem özelinde değerlendirme yapmaktayız.

Gerek bloglarında isimlerini Çince yazıyor olmaları, gerekse isim kökenleri değerlendirildiğinde, grubun Çin menşeli olduğu güvenlik uzmanlarınca iddia edilmektedir[5]. Ayrıca DarkTracer isimli şirket, Tor ağındaki Mount Locker ve Astro Team'e ait domainlerinde host edildiği bilgisine dayandırarak, aynı gruplar olabileceklerini söylemekte.[6]

Xing Team'in 2021 yılında gerçekleştirdiği 21 eyleme sektör ve kıta bazlı baktığımızda büyük oranda Amerika ve Avrupa kıtasında saldırılar düzenlediği görülmektedir. Grubun Asya kıtasında düzenlediği eylemler ise Birleşik Arap Emirlikleri, Suudi Arabistan ve Hindistan ile sınırlıdır. Bu eylemsel davranışı da grubun Çin menşeli olabileceği yönündeki yorumları destekler niteliktedir. Grubun hedef aldığı sektörler arasında üretim, sağlık, enerji, basın yayın, denizcilik, otomotiv gibi birçok farklı sektör göze çarpmaktadır.

Grafik 11: Xing Team'in 2021 yılında gerçekleştirmiş olduğu saldırılara yönelik bilgiler

Grup yukarıdaki grafikte yer verilmiş olan saldırılardan ele geçirmiş olduğu verileri doğrudan paylaşmış durumdadır. Bu durum grubun saldırmış olduğu şirketlerden fidye ödemesi alamadığı yönünde bir değerlendirmeye neden olabilir. Nitekim Xing'in kullanmakta olduğu fidye aracı, birçok özel şirket tarafından "decrypt" edilebilmekte ve veriler kurtarılabilmektedir.

Saldırganların hedef aldığı verilere baktığımızda büyük oranda finansal kayıtlar, kurumsal iletişim kayıtları, personel ve müşteri bilgileri gibi gizlilik derecesi bulunan veriler öne çıkmaktadır.

[5]Andy Greensberg, "Ransomware Struck Another Pipeline Firm—and 70GB of Data Leaked", Wired, https://www.wired.com/story/linestar-pipeline-ransomware-leak/, (Erişim Tarihi: 4.2.2022)
[6] DarkTracer, https://twitter.com/darktracer_int/status/1433694601076822016, (Erişim Tarihi: 4.2.2022)

Türkiye'de hedefli fidye saldırısı gerçekleştirdiği doğrulanan bir diğer grup ise LockBit'tir. Daha önce de ifade edildiği gibi LockBit 2021 yılında en çok hedefli fidye saldırısı gerçekleştiren ikinci gruptur. Uzun yıllardır saldırılarını sürdüren bu grup, kendi TOR ağındaki sitesinde yer verdiği üzere, dünyanın en gelişmiş fidye yazılımını elinde bulundurmaktadır. Bu veriye göre kullandıkları zararlı yazılım, hedef sistemde 100 GB dosyayı 4 dakika 28 saniyede "encrpt" etmektedir. Ayrıca kendi başına sistem içerisinde yayılma kabiliyeti bulunmaktadır. Aşağıdaki grafikte LockBit grubu tarafından gerçekleştirilmiş, kendi zararlı yazılımları da dahil birçok fidye yazılımın kapasitesi yer almaktadır.

LockBit, en gelişmiş zararlı yazılımı kullandığı gibi, dünya genelinde çok sayıda sektörü hedef alması özelliği ile de ekosistemde önemli bir aktör niteliği taşımaktadır. Grubun spesifik bir sektörü hedef almıyor oluşu onun finansal motivasyonlu bir organize suç grubu olduğunu değerlendirmemize yol açmaktadır. Buna karşılık devlet kurumlarını da hedef alıyor olması ve devlet kurumlarının genel olarak fidye ödemeye yanaşmadığı gerçeğiyle birlikte düşünüldüğünde, eylemlerinde espiyonaj niyetinin olduğu yorumu da yapılabilir.

Eylül 2019'dan beri faaliyet yürüten LockBit, diğer birçok hedefli fidye yazılım grubundan saldırı noktasındaki işbirliği program ile ayrılmaktadır. Grup; 3. taraf bir tehdit aktörünün, taraflarına finansal açıdan uygun herhangi bir kuruma ait ana servera erişim imkanı sunduğu taktirde, fidye ödemesinin %8'ini teklif etmektedir. Bu durum grubun dünya genelinde tüm sektörlere nasıl bu kadar fazla saldırı gerçekleştirdiğini açıklama noktasında önemli bir bulgudur.

Grubun saldırılarında izlediği yola baktığımızda açık kaynaklarda bir kuruma ait paylaşılan ya da satılmakta olan önemli bilgileri kullanarak sistemlere erişim yolunu izlemekte. Bunun yanı sıra grup birçok güvenlik zafiyetini de kullanarak sistemlere erişmekte. Australian Cyber Security Centre'ın grup hakkında gerçekleştirdiği bir çalışmaya göre, saldırganlar Fortinet FortiOS ve FortiProxy'lerde bulunan CVE-2018-13379 kodlu zafiyeti istismar ederek birçok şirkete saldırmış durumda.[7]

LockBit bu ve benzeri bir yöntem ile girmiş olduğu sistemde dosyaları şifrelemeden önce, kendi komuta kontrol sunucularına, şirkete ait önemli dosyaları kopyalamakta ve şifreleme işlemini buna müteakip gerçekleştirmektedir. Saldırganların bu ele geçirdikleri verileri kendi kanallarında parça parça yayınlamadan önce, kurbanlarına fidyeyi ödemeleri için genellikle 72 saat gibi bir süre tanımakta.

Ayrıca fidye notlarında her bir şirket için farklı encrypt algoritması kullandıklarını belirtmekte ve herhangi bir şirketin dosyaları tam anlamıyla decrypt edemeyeceğini iddia etmekte. Son olarak Lockbit RaaS hizmeti de sunmasına bağlı olarak TOX ve Jabber üzerinden iletişim sağlamakta.

Türkiye'de 2021 yılında saldırı gerçekleştirmiş olan son grup AvosLocker'a baktığımızda ise; Amerika ve Avrupa kıtasında, özellikle de hizmet sektörünü hedef aldığı görülmektedir. Grubun 2021 yılının ortalarında ortaya çıktığı ve ilk olarak Microsoft Exchange Serverlarda bulunan bir zafiyeti kullanarak hedef şirketlere fidye zararlısı bulaştırdığı tespit edilmiştir. Grup ayrıca illegal forum ve chat kanallarında, iş birliklerine açık olduğunu bildirmektedir. Buna bağlı olarak iletişim için e-posta, XMPP ve TOX kanallarını tercih etmektedir.

[7] ACSC, https://www.cyber.gov.au/sites/default/files/2021-08/2021-006%20ACSC%20Ransomware%20Profile%20-%20Lockbit%202.0.pdf, (Erişim Tarihi: 4.2.2022)

Grubun hedefli fidye zararlısı bulaştırmak için izlediği yöntemlere baktığımızda oltalama saldırıları, dosya paylaşım platformlarında yaydıkları zararlı dosyalar, RDP saldırıları, sahte yazılım güncellemeleri gibi farklı teknikler gözlemlenmektedir. Hedef sisteme bir şekilde sızmayı başardıktan sonra grup "mimikatz" isimli giriş bilgilerini indirmeye yarayan bir araç ile ilgili hedefin kullanıcı adı ve şifrelerini ele geçirmekte ardından da bu bilgiler ile RDP erişimi sağlamaya çalışmaktadır. Sisteme eriştiği durumlarda ise içerde bulduğu dosya ve dokümanları kendi sunucularına kopyalamakta ve daha sonra da arkasında fidye notu ve "avos" uzantılı dosyalar bırakan bir şifreleme yazılımı kullanmaktadır.

Grup başarıyla bir sisteme girebilir ve hedefine ait dosyaları ele geçirmeyi başarır ise bırakmış olduğu fidye notunda, TOR ağlarında bulunan kendi sitelerini ziyaret edilmesi yönünde talimat vermektedir. Ayrıca hedef şirketin dosyaları şifrelendikten sonra en fazla dört gün içerisinde cevap vermelerini talep etmekte, cevap almamaları durumunda fidye fiyatının iki katına çıkacağını, 10'uncu günün sonunda ise ele geçirmiş oldukları tüm veriyi paylaşacaklarını belirtmektedir. Grup 2021'de gerçekleştirmiş olduğu 48 saldırıdan elde ettiği verinin 24'üne ait örnek veriyi kendi platformunda yayınlamış durumdadır. 23 şirkete ait veriyi ise doğrudan satmaktadır.

Encryption speed comparative table for some ransomware - 02.08.2021

PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274 KB	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813 KB	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30 KB	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59 KB	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061 KB	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292 KB	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200 KB	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124 KB	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661 KB	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930 KB	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909 KB	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17 KB	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31 KB	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121 KB	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460 KB	random extension
Avos	18 Jul, 2021	29 MB/s	59M	4D 2H	No	402 KB	79486

Grafik 12: Hedefli fidye saldırısı düzenleyen grupların kullanmakta olduğu zararlılar ve kapasiteleri

SONUÇ VE DEĞERLENDİRME

Hedefli fidye saldırıları uluslararası alanda hem devletler için hem de özel sektörün her alanında faaliyet yürüten şirketler için en önemli siber tehditlerinin başında gelmektedir. 2021 yılında yaşanmış olan 1000'den fazla saldırıyı incelediğimiz bu raporda, tüm sektörlerin ve kurumların hedefli fidye saldırılarına maruz kalma riskiyle karşı karşıya oldukları net bir şekilde görülmektedir. Özellikle birden fazla sektör ile iç içe olan ve iş akış zincirinde yer alan kurumların çok daha büyük bir risk altında olduğu yadsınamaz bir gerçektir.

Pandemi etkilerinin hala devam ettiği, üretim ve hizmette aksaklıkların tüm bir sektöre etki ettiği ve karşılıklı kurumsal bağımlılıkların bu kadar fazla olduğu günümüz dünyasında hedefli fidye saldırısına maruz kalmanın bedeli milyon dolarlar ile ölçülmektedir. Bunun yanında yaşanacak olan itibar ve iş kaybı, özellikle ekonomik daralmaların göründüğü ülkelerde etkisini ve zararını daha büyük hissettirecektir.

Bu bağlamda tüm dünyaya ihracatı her geçen gün artan ve gelişmeye çalışan Türkiye'deki şirketlerin yakın gelecekte en çok maruz kalması beklenen tehditlerin başında hedefli fidye saldırılarını beklemek mümkündür. Özelliklede, 2021 ve öncesinde hedefli fidye saldırısına maruz kalmış olan sektörlere baktığımızda, hizmet, üretim, teknoloji, sağlık, inşaat ve enerji sektörlerinin birincil risk altında olduğu değerlendirilmektedir. Nitekim tüm dünyada hedefli fidye saldırılarının trendi üretim, hizmet, teknoloji, sağlık ve kritik altyapılarda faaliyet yürüten şirketlere doğru yönelmişken, Türkiye'de de durum farklı değildir.

Hedefli fidye saldırılarının genel yapısına baktığımızda, korunmanın mutlak olmadığı ama riskleri azaltmanın ya da devretmenin mümkün olduğu açıktır. Bir hedefli fidye saldırısı çoğunlukla şirkete ait VPN, RDP, kurumsal e-posta gibi yerlere erişimlerin üçüncü bir tehdit aktörü tarafından ihlal edilip illegal kanallarda yayılması ya da satılması ile başlamaktadır. Buna ek olarak her geçen gün ortaya çıkan güvenlik zafiyetleri saldırıya uğramanın açık kapısı gibidir. Son olarak oltalama saldırıları, her türlü hedef odaklı saldırının ana bileşenini oluşturmaktadır.

Haliyle tüm sektörlerin ve şirketlerin siber alandaki varlıklarına yönelik kendileri hakkındaki mevcut verileri ve potansiyel riskleri, istihbari açıdan yakinen takip etmesi bir zorunluluk halini almıştır. Günümüzde birçok siber güvenlik ürünü en az bir saldırının gerçekleşmesi sonrasında koruma mekanizması geliştirmekte iken istihbarat kaynaklarından elde edilecek eyleme dönüştürülebilir tavsiye ve değerlendirmeler, güvenlik mekanizmaları için tamamlayıcı roldedir. Nitekim istihbarat faaliyetleri ile riskler çok daha önceden belirlenerek, tehdit oluşmadan karar alıcılara bildirerek gerekli hazırlık ve önlemlerin alınması amaçlanır.

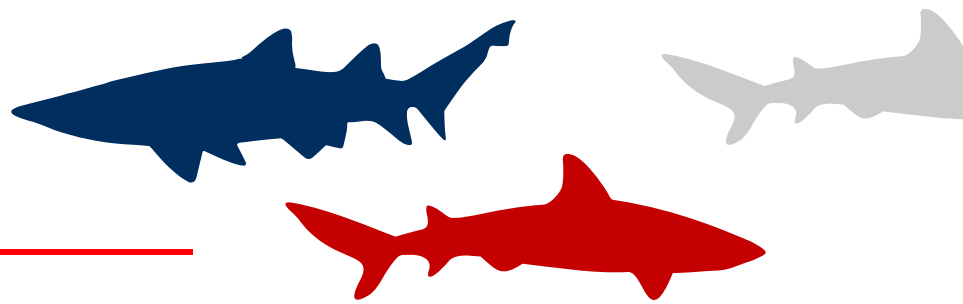
Sonuç olarak; Türkiye'de hedefli fidye saldırıları özelinde gerçekleşebilecek tüm potansiyel saldırıları önlemek için;

- Kurumların tüm açıklarına yönelik kapsamlı OSINT çalışmalarının yapılması ve potansiyel ihlal noktalarının belirlenmesi,
- Siber alandaki varlıklara yönelik güncel zafiyet ve trendlerin sürekli olarak izlenmesi ve ivedilikle önlemlerin alınması,
- Tüm personelin potansiyel riskler hakkında farkındalık kazanması için, gerçek tehditler ile paralellik gösteren simülasyonlar ile eğitilmesi ve bilinçlendirilmesi,

gerekmektedir.

Bunun yanında birçok kurum ve şirketin siber güvenlik konusunda yeterli kaynağı kendi bünyelerinde barındıramadığı da bir gerçektir. Artan saldırı kompleksliği ile birlikte bu saldırılara müdahale etmek için gerekli olan uzmanlığın ve bu uzmanlığın 7x24 esasına göre sağlanması gerekliliği düşünüldüğünde birçok kurumun ve şirketi gelişmiş siber saldırılara karşı tespit ve müdahale hizmeti alması oldukça elzemdir. Yönetilen tespit ve müdahale hizmetleri kapsamında alınacak servisler ile olası siber saldırı girişimlerinin erkenden tespit edilmesi ve bu saldırı girişimlerine müdahalede bulunulması mümkün olmakta, bunu yaparken de her bir kurumun veya şirketin kendi bünyesinde bu uzmanlığı barındırma zorunluluğu ortadan kalmaktadır.

Bu eylemlere ek olarak ulusal siber güvenlik stratejileri bağlamında ilgili devlet kurumlarının alması gereken önlemler ve uygulamalar da söz konusudur. Salt siber güvenlik alanında koordinasyon, strateji ve uygulama geliştiren bir üst otoritenin inşa edilmesi gerekmektedir. Cumhurbaşkanlığı bünyesinde böyle bir kurulun inşa edilmesi ve yönetici pozisyonlarında da teknik ve askeri strateji konularında deneyimleri olan kişilerin bulunması elzemdir. ABD'de Beyaz Saray bünyesinde kurulan Ulusal Siber Direktörlük ve yine İç Güvenlik Bakanlığı'na bağlı olarak inşa edilen Siber Güvenlik İnceleme Kurulu gibi adımlar "siber politika uygulamaları" açısından örnek alınabilecektir.



BAŞVURULAR

Australian Signals Directorate. (2021). 2021-006: ACSC Ransomware Profile- Lockbit 2.0. Australian Government.

Chainalysis. (2021). The 2021 Crypto Crime Reports.Chainalysis.

DarkTracer. (tarih yok). https://twitter.com/darktracer_int/status/1433694601076822016 adresinden alındı

Greensberg, A. (2021, 6 7). Ransomware Struck Another Pipeline Firm—and 70GB of Data Leaked. Wired: https://www.wired.com/story/linestar-pipeline-ransomware-leak/ adresinden alındı

Ransom-DB. (2021). Ransomware Database. random-db: https://www.ransom-db.com/ransomware-statistics adresinden alındı

U.S. Department of the Treasury. (2021). Treasury Continues to Counter Ransomware as Part of Whole of Government Effort: Sanctions Ransomware Operators and Virtual Currency Exchange. Washington: U.S. Department of the Treasury.

www.adeo.com.tr

ADEO Cyber Security Services
@adeocomtr
@adeocomtr
ADEOcomtr
@adeocomtr

İSTANBUL
Fetih Mah. Tahralı Sk.
Tahralı Sitesi Kavakyeli Plaza
C Blok D16/17
Ataşehir / İSTANBUL / TÜRKİYE
Telefon: +90 (216) 472 35 35
Fax : +90 (216) 472 35 36
Email: info@adeo.com.tr

ANKARA
Kabil Cad.(Eski 4.Cad)
1335. Sokak No:58 D:9-10
Aşağı Öveçler
Çankaya / ANKARA / TÜRKİYE
Telefon: +90 (312) 482 12 35
Fax : +90 (312) 482 12 36
Email: ankara@adeo.com.tr

www.adeo.com.tr