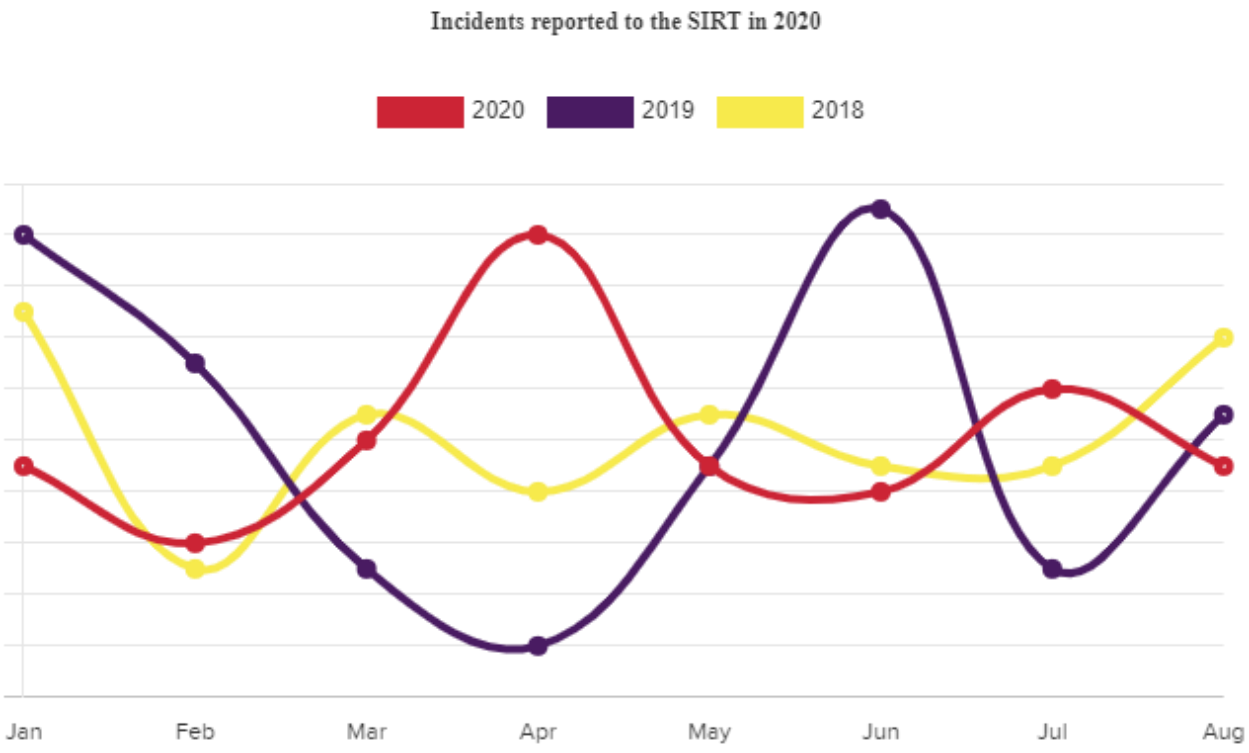
https://www.f5.com/labs/articles/threat-intelligence/how-cyber-attacks-changed-during-the-pandemic

Pandemi Sürecinde, Siber Saldırılardaki Değişimin Farkında Mısınız?

F5 Networks Güvenlik Vaka Müdahale Ekibi (F5 SIRT), kullanıcıların siber güvenlik konusunda karşılaştıkları vakaları gerçek zamanlı ele alarak, onlara yardımcı olur.
F5 SIRT Ekibimiz, bu çalışmayı hazırlarken pandeminin siber saldırıları nasıl değiştirdiğini incelemek için, 2020 yılbaşından Ağustos ayına kadar bildirilen tüm vakaları gözden geçirdi. Müşteri gizliliği kapsamında, isim ve bazı rakamları açıklayamıyoruz; ancak tüm dünyada karşılaşılan durumlarla ilgili, öngörü sağlaması için, raporlardaki artış seviyelerini gözler önüne seriyoruz.

Pandemi Sürecinde, Siber Saldırılarda Artış Yaşandığını Biliyor Musunuz?

Araştırmamızda, Mart 2020'de pandemi sebebiyle eve kapanma döneminin başlangıcında bildirilen vakalarda daha önce görülmemiş bir artış yaşandığını tespit ettik. Başlangıçta, Ocak ayında raporlanan vakaların sayısı, önceki yıllara göre düşük seyrediyordu. Mart ayında salgından dolayı yasaklar uygulanmaya başladıkça, güvenlik tehdit bildirimlerinde de, belirgin bir şekilde artış gözlendi. Nisan ayına geldiğimizde önceki yıllara göre, güvenlik tehdit bildirimleri 3 kat artışla zirve yaptı. Mayıs ve Haziran aylarında durum normale dönmeye başladı. Ancak, rakamlar Temmuz ayında, 2019 yılının, 2 katına ulaştı. Aşağıdaki grafik, son 3 yılda Ocak- Ağustos döneminde, raporlanan siber saldırıları göstermektedir.



2018-2020 için, Ocak'tan Ağustos'a kadar F5 SIRT'e raporlanan güvenlik vakaları.

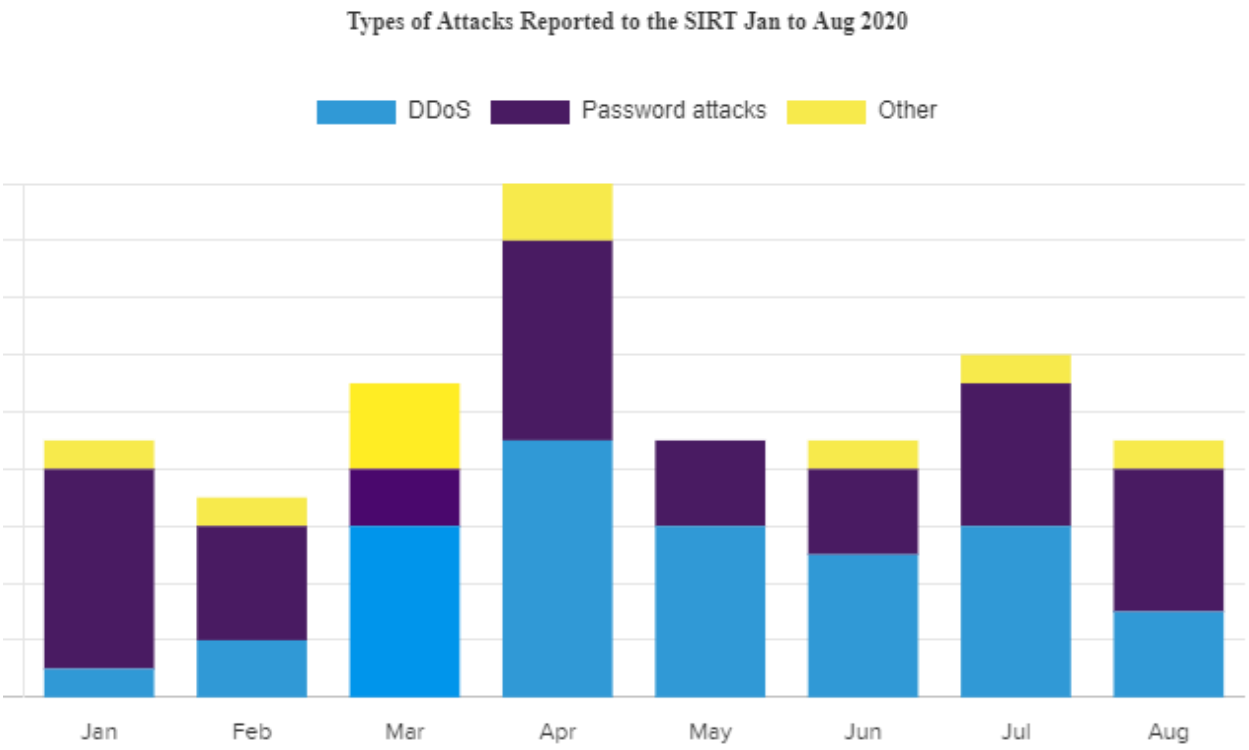
DDoS: Distributed Denial of Service

F5 SIRT'a Bildirilen Vakalar Neydi?

Bildirilen güvenlik vakaları ifadesi, kullanıcıların F5 SIRT'ten destek istediği, çeşitli siber saldırı türlerini ifade eder. Öncelikle, bu siber saldırılar 2 gruba ayrıldı: Dağıtılmış Hizmet Reddi (DDoS) ve şifre girişi saldırıları. Parola giriş saldırıları ve kimlik bilgisi doldurma saldırılarından oluşuyordu. Bunların her ikisi de, siber saldırganların herhangi bir şifre girişini, geçme yollarını tahmin etmeyi içerir. (Password login attacks; Brute Force; Credential Stuffing attacks)

Ocak- Ağustos döneminde, bildirilen güvenlik olaylarının %45'i DDoS ve%43'ü şifreli giriş saldırılarından oluşuyordu. Bildirilen güvenlik olaylarının geri kalan %12'si kötü amaçlı yazılım bulaşması, web saldırıları veya sınıflandırılmamış saldırılardı.

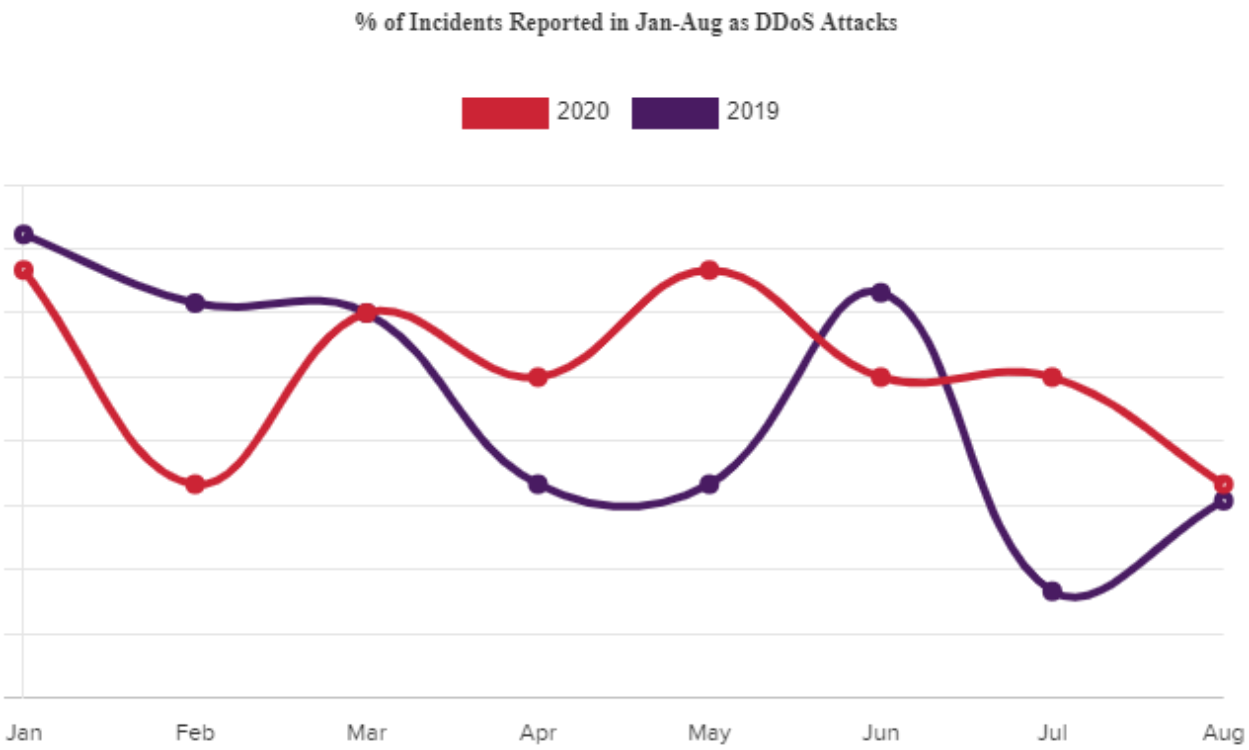
Şekil 2'de görüldüğü gibi DDoS saldırıları, pandemi sürecinde, eve kapanma dönemindeki vakalarda hakim oldu. DDoS saldırıları, Ocak ayında raporlanan vakaların sadece 1/10'unu oluşturuyordu; ancak daha sonra Mart'taki tüm vakaların 3 katına çıktı. Sonraki süreçte, DDoS, sürekli olarak en yüksek seviyede seyretmiştir.



Şekil 2. Ocak - Ağustos 2020 F5 SIRT'e bildirilen siber saldırı türleri

DDoS: Distributed Denial of Service

DDoS* kısaltmasındaki D harfi, dağıtılmış anlamına gelir. DDoS saldırılarının, dünya çapında güvenliği ihlal edilmiş makinelerin büyük botnet'lerinden kaynaklandığını ifade eder. Geçmiş yıllara göre, DDoS saldırılarında bir “bahar düşüşü” yaşandı; ancak bu yıl Nisan ayından itibaren büyük bir artışa şahit olduk, sadece Haziran'da hafif bir düşüş oldu. Yıllık ortalamada, rakamlar birbirine benzerdir ve raporlanan vakalar 2019'da %46 iken; 2020'de %51’i DDoS olarak gerçekleşmiştir. Bununla birlikte, DDoS saldırılarının aylık zamanlaması, Şekil-3'de gösterildiği gibi eve kapandığımız dönemde farklı bir şekilde seyretmiştir.



Şekil 3. F5 SIRT'e DDoS olarak bildirilen olayların yüzdesi Ocak - Ağustos 2019 ve 2020

Bu dönemde, Rus siber saldırgan Fancy Bear kaynaklı olduğu iddia edilen, tehdit girişimlerinden bahsetmemiz gerekir. Öncelikle küçük bir DDoS saldırısıyla başladı ve ardından yüz binlerce dolarlık bir ödeme talebi geldi. Ödeyin, aksi takdirde "siz ödeme yapana kadar hizmetleriniz çevrimdışı kalacaktır." Uyarısı yapıldı. İlginç olan nokta, Fancy Bear'ın DDoS saldırıları veya tehditle tanınmayan bir siber casusluk grubu olması, Fancy Bear, daha çok casusluk ve politik amaçlarla saldırı yapan bir grup olarak biliniyor. Gerçek Fancy Bear'ın bu son atakları gerçekleştirmesi pek olası görünmüyor. .

2020'de DDoS Saldırı Türlerindeki Değişim

Genel olarak, bildirilen DDoS saldırılarının çoğu hacimseldir, yani ağ bant genişliğini hedefler ve kullanıcılar için, bağlantıları engellemeye yönelik gereksiz paketlerle doldurur. Bunu yapmanın yaygın bir yöntemi, DNS isteklerini hedefe geri saldırmak için, taklit eden bir DNS Flood saldırısıdır. 2019'da, F5 SIRT'e bildirilen tüm DDoS saldırılarının %17'si DNS amplifikasyon saldırıları olarak tanımlandı. Ancak 2020'de bu sayı neredeyse 2’ye katlanarak %31'e yükseldi.

DDoS: Distributed Denial of Service

Diğer bir DNS DDoS saldırı tekniği, bir saldırganın, bir DNS sunucusunun kaynaklarını bitirmesi için, kasıtlı olarak hatalı biçimlendirilmiş, kötü amaçlı DNS istekleri gönderdiği bir DNS sorgu taşmasıdır. 2020'de DDoS saldırılarının %12'si müşteri DNS sunucularına yönelik kötü niyetli DNS istekleriydi.

2020'nin ilk yarısı, web sitelerini ve uygulamaları hedef alan DDoS saldırılarında da artış görüldü. 2019'da, F5 SIRT'e bildirilen DDoS saldırılarının% 4,2'sinin web uygulamalarını hedeflediği belirlendi. Ancak bu rakam, 2020'de 6 kat artarak %26'ya yükseldi.

F5 SIRT olay verileri ayrıca saldırı türünde coğrafi farklılıkları ortaya çıkardı. Asya / Pasifik bölgesi, dünya genelindeki en yüksek oran olan %83 olarak, DDoS'u bildirildi. F5 SIRT'e bildirilen olayların DDoS saldırıları olarak raporlandığı bölgeler içinde, sonraki en yüksek oran ise, %54 ile Avrupa, Orta Doğu ve Afrika (EMEA) bölgesi oldu.

Şifre Giriş (Access Attacks) Saldırılarındaki Değişiklikler

Kimlik bilgilerini doldurma ve Brute Force, internetteki başlıca tehditlerdir. Pandemi, fiziksel olarak mağaza içi satın almadan elektronik ticarete geçişe neden olurken, perakende sektöründe, şifre saldırıları gerçekleşmesini beklemek kaçınılmazdı. Gerçekten de, 2020'de perakendecilere yönelik F5 SIRT tarafından bildirilen saldırıların % 67'si şifre saldırılarıydı; bu oran 2019'da sadece % 40'tı. Ayrıca 2020'de, servis sağlayıcılardan gelen vaka raporlarının yarısı şifre girişi saldırılarıyla ilişkilendirildi. Finansal hizmet müşterileri de, gerçekleşen vakaların %43'ünü şifre girişi olarak bildirdi.

F5 Labs ayrıca, parola giriş saldırıları tarafından saldırıya uğrayan, belirli teknik hizmet türlerine de göz kulak olur. Büyüme alanlarından biri, API'lere yönelik kimlik doğrulama saldırılarıdır ve F5 SIRT raporları, 2019'da %2,6'dan 2020'de şu ana kadar % 5'e, iki katına çıkmıştır.

DDoS: Distributed Denial of Service