11.10.2021

BİLGİSAYAR MÜHENDİSLİĞİ TASARIMI RAPORU

Zararlı Yazılım Analizi

Zararlı Yazılım Nedir?

Zararlı yazılım, programlanabilir herhangi bir aygıta, hizmete veya ağa zarar vermek veya bunlardan yararlanmak üzere tasarlanmış her türlü zararlı yazılım için kullanılan kapsamlı bir terimdir. Siber suçlular genellikle bunu, mali kazanç için kurbanlardan veri elde ederek baskı yapmak üzere kullanır. Bu veriler finansal verilerden sağlık kayıtlarına, e-postalara ve parolalara kadar değişebilir. Zararlı yazılımlar büyük küçük firmalara ve herhangi bir kullanıcıya karşı oldukça tehlikeli silahlara dönüşebilirler. Bu nedenle zararlı yazılımların tespiti ve incelenmesi oldukça önem arz eden bir konudur. Bu raporda zararlı yazılım ile ilgili daha detaylı bilgiler paylaşacağım.

Zararlı Yazılım Türleri Nelerdir?

Zararlı yazılımlar kendi içerisinde çok sayıda çeşidi vardır. Temel başlık olarak incelenen çeşitleri daha detaylı bir şekilde incelemeyerek araştırma yaptım ve raporu aşırı fazla uzatmadan başlıklar halinde raporun devamında paylaştım.

1. Bilgisayar Virüsleri Nelerdir?

Virüs, çalıştırıldığında diğer bilgisayar programlarını değiştirerek ve kendi kodlarını ekleyerek kendi kendini kopyalayan bir kötü amaçlı yazılım türüdür. Bu çoğaltma başarılı olduğunda, etkilenen bölgelere virüs bulaştığı söylenir. Virüs yazarları sosyal mühendisliği kullanır ve sistemlere bulaşmak ve virüsü yaymak için güvenlik açıklarından yararlanır. Windows ve Mac işletim sistemleri, virüsten koruma yazılımlarından kaçınmak için genellikle karmaşık algılama önleme stratejileri kullanan virüslerin büyük çoğunluğunun hedefleridir. Virüsler kar elde etmek (fidye yazılımı vb.), mesaj göndermek, kişisel eğlence, güvenlik açıklarının var olduğunu göstermek, sabote etmek ve hizmet reddini göstermek veya sadece siber güvenlik sorunlarını, yapay yaşamı ve evrimsel algoritmaları keşfetmek için yaratılmıştır. Bilgisayar virüsleri, sistem arızasına, kaynak israfına, verilerin bozulmasına, bakım maliyetlerinin artmasına, tuş vuruşlarının kaydedilmesine ve kişisel bilgilerin çalınmasına (kredi kartı numaraları vb.) neden olarak milyarlarca dolar değerinde ekonomik hasara neden olur.

2. Bilgisayar Solucanı Nedir?

Bir bilgisayar solucanı, birincil amacı virüslü sistemlerde aktif kalırken kendisini kopyalayarak diğer bilgisayarlara bulaşmak olan kendi kendini kopyalayan bir kötü amaçlı yazılım programıdır. Genellikle solucanlar, erişmek için hedef bilgisayardaki güvenlik açıklarına veya güvenlik hatalarına güvenerek yaymak için bilgisayar ağlarını kullanır. Solucanlar, yalnızca bant genişliği tüketerek bile olsa, neredeyse her zaman bir ağa en azından bir miktar zarar verir. Bu, kurbanın bilgisayarındaki dosyaları neredeyse her zaman bozan veya değiştiren virüslerden farklıdır. WannaCry, EternalBlue güvenlik açığından yararlanarak kullanıcı eylemi olmadan yayılan bir fidye yazılımı cryptoworm'un ünlü bir örneğidir. Birçok solucan yalnızca yayılacak ve geçtikleri sistemleri değiştirmeyecek şekilde tasarlanırken, yük taşımayan solucanlar bile büyük aksamalara neden olabilir. Morris solucanı ve Mydoom, iyi huylu doğalarına rağmen ağ trafiğini artırarak büyük aksaklıklara neden olmaktadırlar.

3. Truva Atı (trojan) Nedir?

Truva atı veya truva atı, meşru bir programmış gibi davranarak kullanıcıları gerçek niyetinden saptıran herhangi bir kötü amaçlı yazılımdır. Bu terim, Truva kentinin yıkılmasına yol açan aldatıcı Truva Atının Antik Yunan hikayesinden türetilmiştir. Truva atları genellikle kimlik avı gibi sosyal mühendislik ile yayılır. Örneğin, bir kullanıcı orijinal görünecek şekilde gizlenmiş bir e-posta eki çalıştırması için kandırılabilir (örn. Bir Excel elektronik tablosu). Yürütülebilir dosya açıldıktan sonra truva atı yüklenir. Bir truva atının yükü herhangi bir şey olabilirken, çoğu saldırgana virüslü bilgisayara yetkisiz erişim sağlayan bir arka kapı görevi görür. Truva atları, internet etkinliği, bankacılık oturum açma kimlik bilgileri, parolalar veya kişisel olarak tanımlanabilir bilgiler (PII) gibi kişisel bilgilere erişim sağlayabilir. Fidye yazılımı saldırıları da truva atları kullanılarak gerçekleştirilir. Bilgisayar virüsleri ve solucanlardan farklı olarak truva atları genellikle diğer dosyalara kötü amaçlı kod enjekte etmeye veya kendilerini yaymaya çalışmazlar.

4. Rootkitler nelerdir?

Rootkit, bir bilgisayara veya yazılım alanına yetkisiz erişim sağlamak için tasarlanmış ve genellikle varlığını veya başka bir yazılımın varlığını maskeleyen bir kötü amaçlı yazılım topluluğudur. Rootkit yüklemesi otomatikleştirilebilir veya saldırgan bunu yönetici erişimi ile yükleyebilir. Erişim, güvenlik açıklarından yararlanma, parola kırma veya kimlik avı gibi sisteme yapılan doğrudan bir saldırı sonucu elde edilebilir. Rootkit tespiti zordur çünkü onu bulmak için tasarlanan virüsten koruma programını altüst edebilir. Algılama yöntemleri arasında güvenilir işletim sistemlerinin kullanılması, davranışsal yöntemler, imza taraması, fark taraması ve bellek dökümü analizi yer alır. Rootkitlerin kaldırılması, özellikle rootkitler çekirdekte bulunduğunda karmaşık veya pratik olarak imkansız olabilir. Ürün yazılımı rootkitleri donanım değişimi veya özel donanım gerektirebilir.

5. Fidye Yazılımı (Ransomware) nedir?

Fidye yazılımı, fidye ödenene kadar bir bilgisayar sistemine veya verilere erişimi reddetmek için tasarlanmış bir kötü amaçlı yazılım biçimidir. Ransomware e-postalar, malvertising(kötü amaçlı) ziyaret enfekte Kimlik Avı web sitelerinin güvenlik açıklarını istismar ederek yayılır. Fidye yazılımı saldırıları kesinti sürelerine, veri sızıntılarına, fikri mülkiyet hırsızlığına ve veri ihlallerine neden olur. Fidye ödeme tutarları birkaç yüz ila yüz binlerce dolar arasında değişmektedir. Bitcoin etherium gibi izlenemeyen kripto para birimleriyle ödenmektedir.

6. Keylogger nedir?

Keyloggerlar, klavyede basılan karakterleri kaydetmek ve izlemek için kullanılan bir kötü amaçlı yazılım türüdür. Keyloggerlar akıllı telefonlar için de kullanılabilir. Keyloggerlar toplanan bilgileri depolar ve daha sonra oturum açma kimlik bilgileri ve kredi kartı bilgileri gibi hassas bilgileri çıkarabilen saldırgana gönderir.

7. Grayware nedir?

Grayware terimi Eylül 2004'te kullanılmaya başlandı ve kötü amaçlı yazılım olmayan ancak bilgisayarın performansını kötüleştiren ve siber güvenlik riskine neden olabilecek istenmeyen uygulamaları veya dosyaları tanımlar. Casus yazılım/Grayware, virüsler veya truva atları olarak sınıflandırılmayan, ancak yine de ağınızdaki son noktalar performansını olumsuz olarak etkileyen ve kuruluşunuza önemli güvenlik, gizlilik ve hukuki tehlikeler doğuran uygulamalar veya dosyalar için kullanılır. Casus yazılım/grayware genellikle açılır pencerelerle, kullanıcıların bastığı tuşları kaydederek ve son nokta güvenlik açıklarını saldırıya maruz bırakarak kullanıcıları sinirlendirmek gibi istenmeyen ve tehdit edici eylemler gerçekleştirir. Grayware'in bilgisayara erişmek için kullandığı

mekanizma, sosyal mühendislik, eşleştirilmemiş yazılım veya diğer güvenlik açıkları olsun fidye yazılımı gibi diğer kötü amaçlı yazılım türleri de erişmek için de aynı yöntemi kullanabilir.

8. Fileless Malware nedir?

Fileless malware, bir cihaza bulaşmak için hedefe yeni bir yazılım yüklemek yerine cihazdaki mevcut yazılımları (Ör: PowerShell) kötü amaçlı kullanan yazılımlardır. Direkt olarak hedef sisteme dosya yüklemez ve RAM üzerinde çalışır. Bu yönlerinden dolayı herhangi imza tabanlı bir antivirüs sistemi tarafından tespit edilemez. Dosyasız kötü amaçlı yazılım, bir bilgisayara bulaşmak için meşru programlar kullanan bir kötü amaçlı yazılım türüdür. Diğer kötü amaçlı yazılım bulaşmalarından farklı olarak, dosyalara güvenmez ve ayak izi bırakmaz, bu da kötü amaçlı yazılım önleme yazılımının algılamasını ve kaldırmasını zorlaştırır. Yalnızca bilgisayar belleği tabanlı bir eser olarak, yani ram'de bulunur.Dosyasız kötü amaçlı yazılım, 2017'de ana siber tehdit olarak ortaya çıktı, ancak bir süredir var. Frodo, Canavarın Sayısı ve Karanlık İntikamcı hepsi erken dosyasız kötü amaçlı yazılım saldırılarıydı. Daha yakın zamanlarda, Demokratik Ulusal Komite ve Equifax ihlali, dosyasız kötü amaçlı yazılım saldırılarına kurban gitti. Fileless kötü amaçlı yazılım varolan anti dayanıklı dosya eklemek için adli bilişim stratejileri, beyaz liste damgalama, imza algılama, donanım doğrulama, desen analizi veya zaman tabanlı yapma--bilgisayar sabit diskine faaliyetlerini herhangi bir bölümünü yazmaz. Dijital adli tıp araştırmacıları tarafından gayri meşru faaliyetleri tespit etmek için kullanılabilecek çok az kanıt bırakıyor. Bununla birlikte, bellekte çalışmak üzere tasarlandığından, genellikle yalnızca sistem yeniden başlatılıncaya kadar var olur.

9. Adware nedir?

Adware, genellikle bir web tarayıcısında veya açılır pencerede ekranınıza reklam yerleştirmek için tasarlanmış bir tür gri yazılımdır. Genellikle, bilgisayarınıza, tabletinize veya akıllı telefonunuza yüklemeniz için sizi kandırmak için kendisini başka bir programdaki meşru veya piggybacks olarak ayırır. Adware, en karlı, en az zararlı kötü amaçlı yazılım biçimlerinden biridir ve mobil cihazlarda giderek daha popüler hale gelmektedir. Adware, yazılımın kullanıcısına otomatik olarak reklam görüntüleyerek gelir elde ettirir.

10. Malvertising nedir?

Kötü amaçlı reklamların bir birleşimi olan Malvertising, kötü amaçlı yazılımları yaymak için reklamın kullanılmasıdır. Genellikle kötü amaçlı veya kötü amaçlı yazılım yüklü reklamların meşru reklam ağlarına ve web sayfalarına enjekte edilmesini içerir. Önemli çaba reklamları satmak ya da bir ürün tanıtımı kullanıcıları çekmek için onları koymak için reklam kötü amaçlı yazılım yaymak için harika bir yoldur. Malvertising, yüksek profilli ve saygın haber siteleri gibi yerleştirildiği sitelerin itibarından da yararlanmaktadır.

11. Virüs nedir?

Casus yazılım, bir kişi veya kuruluş hakkında bazen bilgisi olmadan bilgi toplayan ve bilgileri mağdurun rızası olmadan saldırgana gönderen kötü amaçlı yazılımdır. Casus yazılımlar genellikle internet kullanım verilerinizi izlemeyi ve satmayı, kredi kartı veya banka hesap bilgilerinizi yakalamayı veya kişisel olarak tanımlanabilir bilgileri (PII) çalmayı amaçlar. Bazı casus yazılım türleri ek yazılım yükleyebilir ve cihazınızdaki ayarları değiştirebilir. Casus yazılımların kaldırılması genellikle kolaydır, çünkü diğer kötü amaçlı yazılım türleri kadar kötü değildir.

12. Botlar ve Botnetler nedir?

Bir bot, bir saldırgan tarafından uzaktan kontrol edilmesini sağlayan kötü amaçlı yazılım bulaşmış bir bilgisayardır. Bot (veya zombi bilgisayar) daha sonra daha fazla siber saldırı başlatmak veya bir botnetin (bir bot koleksiyonu) parçası olmak için kullanılabilir. Botnetler dağıtılmış hizmet reddi(DDoS) saldırıları, fidye yazılımı yayma, keylogging ve diğer kötü amaçlı yazılım türlerini yayma için popüler bir yöntemdir.

13. Arka Kapı(backdoor malware) nedir?

Arka kapı, bir sisteme erişmek için normal kimlik doğrulama prosedürlerini reddeden bir kötü amaçlı yazılım türüdür. Sonuç olarak, bir uygulama içindeki veritabanları ve dosya sunucuları gibi kaynaklara uzaktan erişim verilir ve faillere uzaktan sistem komutları verme ve kötü amaçlı yazılımları güncelleme yeteneği verir. Arka kapı; bir bilgisayarda, üründe, gömülü aygıtta (örn. Yönlendirici) veya bilgisayarın başka bir bölümünde normal kimlik doğrulama veya şifrelemeyi atlamak için kullanılan gizli bir yöntemdir. Arka kapılar genellikle bir bilgisayara uzaktan erişimi güvence altına almak veya şifrelenmiş dosyalara erişmek için kullanılır. Buradan hassas verilere erişmek, bozmak, silmek veya aktarmak için kullanılabilir. Arka kapılar, bir programın gizli bir parçası (truva atı), bellek ve işletim sistemlerinde ayrı bir program veya kod şeklinde olabilir. Ayrıca, arka kapılar oluşturulabilir veya yaygın olarak bilinir. Birçok arka kapı, üreticinin kullanıcı şifrelerini sıfırlamanın bir yoluna ihtiyaç duyması gibi meşru kullanım durumlarına sahiptir.

Zararlı Yazılım Analizi Nedir?

Zararlı yazılım analizi, şüpheli bir dosyanın veya URL'nin davranışını ve amacını anlama sürecidir. Analizin çıktısı, potansiyel tehdidin tespit edilmesine ve azaltılmasına yardımcı olur. Zararlı yazılım analizinin en büyük faydası, olaya müdahale eden siber güvenlikçilere ve IT ekiplerine oldukça yardımcı olmasıdır.

Zararlı Yazılım Analiz Çeşitleri

Zararlı yazılım analizleri Statik, Dinamik ve hibrit (statik ve dinamik birlikte) olacak şekilde 3 farklı teknik ile gerçekleştirilir. Ayrıca son yıllarda popülerleşen bellek analizi de bu teknikler arasına dahil edilmiştir. Statik analiz, zararlının çalıştırılmadan, hızlı bir şekilde hakkında bilgi toplanmasına verilen isimdir. Dinamik analiz ise zararlı yazılımı zafiyetli makine gibi cihazlarda çalıştırarak yazılımın amaçlarını öğrenebilmemizi sağlar.

1.Statik Analiz

Statik analizde kullanılabilecek ilk araç olan “virustotal”, elimizdeki zararlı yazılımın imza tabanlı araştırmasını yapabileceğimiz bir platformdur. Yazılımın daha önceden bir imza veri tabanında bulunup bulunmadığını kontrol edebilir. Ardından yazılımın içerdiği stringlere bakarak hangi kütüphaneleri, DLL’leri vs. kullandığını görebilmekteyiz. Zararlı yazılım yüksek ihtimalle paketlenmiş veya obfuscation (kod karmaşıklaştırma) yapılmış olarak karşımıza çıkmaktadır. Örneğin, bir dosya daha sonra dinamik dizeye dayalı olarak kötü amaçlı bir dosya indiren bir dize oluştururursa, temel bir statik analiz tarafından algılanmayabilir. Siber güvenlikçiler büyük ve küçük şirketler, dosyanın davranışını daha eksiksiz anlamak için dinamik analize yönelmektedir.

2.Dinamik Analiz

Dinamik kötü amaçlı yazılım analizi, şüpheli kötü amaçlı kodları sandbox adı verilen güvenli bir ortamda yürütür. Bu kapalı sistem, güvenlik uzmanlarının sistemlerine bulaşmasına veya kurumsal ağa kaçmasına izin verme riski olmadan kötü amaçlı yazılımları eylem halinde izlemelerini sağlar. Dinamik analiz, tehdit avcılarına ve olay müdahalecilerine daha derin görünürlük sağlayarak bir tehdidin gerçek doğasını ortaya çıkarmalarını sağlar. İkincil bir avantaj olarak, sandboxlardaki kötü amaçlı kodu bulmak için bir dosyayı tersine mühendislik yaparak harcanması gereken süreyi ortadan kaldırır.

3.Hibrit Analiz (Karma analiz. Diğer iki tekniği de içinde barındırır)

Statik analiz (Temel), karmaşık kötü amaçlı kodları tespit etmenin güvenilir bir yolu değildir ve karmaşık kötü amaçlı yazılımlar bazen sandbox (sanal alan) teknolojisinin varlığından gizlenebilir. Temel ve dinamik analiz tekniklerini birleştirerek gerçekleştirilen bu karma analiz, güvenlik ekibine her iki yaklaşımın da en iyisini sunar; çünkü öncelikle gizlemeye çalışan kötü amaçlı kodları algılayabilir ve daha sonra statik olarak daha önce görünmeyen kodlarla daha birçok uzlaşma göstergesini (IOC) çıkarabilir. Hibrit analiz, en gelişmiş kötü amaçlı yazılımlardan bile bilinmeyen tehditleri tespit etmeye yardımcı olur. Örneğin, karma analizin yaptığı şeylerden biri, davranış analizi tarafından oluşturulan verilere statik analiz uygulamaktır. Bir parça kötü amaçlı kod çalıştırıldığında ve bellekte bazı değişiklikler oluşturduğunda, dinamik analiz bunu algılayacak ve analistler geri dönüp bu bellek dökümü üzerinde temel statik analiz yapmaları konusunda uyarılacak. Sonuç olarak, daha fazla IOC üretilecek ve sıfır gün saldırıları (zero-day exploit) ortaya çıkacaktır.

Yasin ALTUNBAŞAK