Rootkit Nedir? Rootkit Programlama ve Rootkit Virüsü

Rootkit, bilgisayarın işletim sistemi çekirdeğine sızarak kötü niyetli kişilere bilgisayarınızı uzaktan kontrol etme ve tam yetki sağlayan virüs türevi zararlı yazılımlardır. Rootkit yazılımları genellikle Unix ve Linux türevi işletim sistemleri ve Windows işletim sistemi için geliştirilir.

Rootkit yazılımlarını standart virüs yazılımlarıyla karıştırmamalısınız. Virüs yazılımlarının amacı bilgisayarınıza yerleştikten sonra kendini çoğaltmak ve sistemin tamamını sararak sistemden faydalanmaktır. Oysa Rootkit programlarının amacı kendini sisteme saldıktan sonra çoğaltmak değil, doğrudan uzaktaki kötü niyetli kullanıcılara bilgisayarınız üzerinde tam kontrole sahip olma şansı sunmaktır.

Tüm bu detayları göz önüne alacak olursak bir Rootkit, standart virüslere oranla çok daha fazla tehlikelidir. Rootkit yazılımlarının hemen hemen tümü kendini işletim sisteminin çekirdek bölümüne gizler ve bu sayede Antivirüs yazılımları tarafından fark edilmeden işlevlerini yerine getirebilir.

Rootkit Programlama

Rootkit oluşturmak bilgisayar teknolojileri, güvenlik, bilgisayar ağları ve çeşitli yazılım dilleri konusunda ciddi tecrübe isteyen bir iştir. Zira Rootkit yazılımlar diğer virüslerle karşılaştırıldığında çok daha etkili işlevlere sahiptir ve bunlar planlanması için Rootkit programlayacak kişinin ne yaptığının farkında olması ve hedef sistemin inceliklerini yeterince tanıyor olması gerekir. Oluşturduğunuz bir Rootkit'i izinsiz şekilde farklı birinin bilgisayarına yerleştirmek bilişim hukuku gözünde çok ciddi bir suçtur ve ağır hapis cezasıyla cezalandırılabilir.

Rootkit Virüsü

Bilgisayar virüslerinin tamamı bir amaç için sistem üzerinde yer alırlar. Oysa Rootkit'ler tam olarak bilgisayar virüsü değillerdir. Bilgisayar virüsü olmamalarına karşın Rootkit yazılımları virüslerden çok daha tehlikelidir. Rootkit bilgisayarınızın sistemine yerleştikten sonra Rootkit'in yöneticisi bilgisayarınız üzerinde tam yetki sahibi haline gelir. Dolayısıyla internet korsanı Rootkit'i başarıyla sisteminize yerleştirdikten sonra;

Bilgisayarınızda kullandığınız hesapları ele geçirebilir.

Banka ve kredi kartı bilgilerinize erişebilir.

Bilgisayarınız üzerindeki erişebilir tüm dosyaları görüntüleyebilir ve hatta bu dosyaları kendi bilgisayarına transfer edebilir.

Sizin bilgisayarınız üzerinden sanal saldırılar gerçekleştirebilir.

Bilgisayarınızı Botnet veya DDoS saldırılarının bir parçası haline getirebilir.

Bilgisayarınız üzerinden yasa dışı işlemler gerçekleştirebilir.

Web kamerası, mikrofon vb. tüm donanımlarınızı kullanarak kişisel gizliliğinizi ihlal edebilir.

Peki, sistemimizin içerisinde bir Rootkit'in yer alıp almadığını nasıl anlayabiliriz? Bilgisayarınıza bir Rootkit giriş yaptığında bunu muhtemelen anlayamayacaksınız. Rootkit'ler doğrudan sistemin içerisine sızdıkları için antivirüs yazılımları tarafından yakalanmayacaktır. Rootkit yazılımın sisteminizde var olup olmadığını öğrenmek için antivirüs ve güvenlik firmaları tarafından geliştirilen ücretsiz Rootkit tarama yazılımlarını indirerek bilgisayarınızda tarama işlemleri gerçekleştirebilirsiniz.

Rootkit virüsleri oldukça zararlı virüslerdir fakat bunların sisteme bulaşması çoğunlukla kullanıcıların kendi hataları veya gösterdiği güvenlik zafiyetlerinin bir sonucudur. Sisteminizi Rootkit virüslerinden uzak tutmak için;

Yasal olmayan hiçbir web sitesine giriş yapmayın ve yasal olmayan şeyleri indirmeyin.

Kullandığınız yazılım veya işletim sistemlerini yasal olmayan yollarla elde etmek için crack, keygen veya acitvator yazılımlar kullanmayın.

Kullanacağınız yazılımları aracı siteler yerine doğrudan resmi kaynaklarından indirmeye çalışın.

Sisteminizde Rootkit denetlemesi yapabilecek bir güvenlik yazılımı edinin.

Fidye yazılımı nedir?

Fidye yazılımı nedir?
Fidye yazılımı, her geçen gün gelişen ve daha da yaygınlaşan bir zararlı yazılımdır.
Temelde iki türü vardır: şifreleyiciler ve kilitleyiciler.

Bilgisayarınıza şifreleyici bulaştığı zaman, bilgisayarınızda bulunan her türlü veriyi (dosyalar, fotoğraflar, oyunların save dosyaları, veri tabanları vs.) şifreler. Dosyalar bir defa şifrelendiğinde dosyaları açamazsınız ve dosya içerisinde bulunan verilere ulaşamazsınız. Bu saldırıları düzenleyen suçlular dosyalarınızı açabilecek özel anahtar karşılığından fidye talep ederler. Talep edilen ortalama fidye miktarı 300$ civarıdır.

Diğer türe kilitleyici denilmesinin sebebi ise, bu zararlı yazılımların bütün cihazı kilitlemesi. Yani sadece dosyalarınız değil, bütün sisteminiz erişilmez olur. Ama tuhaftır, kilitleyicilerin istedikleri fidye miktarı şifreleyicilerinki kadar yüksek değil.

Niye fidye yazılımları hakkında bilgilenmeniz gerekiyor
Öncelikle, piyasada çok sayıda fidye yazılımı mevcut. Tüm Windows, Mac OS X, Linux ve Android cihazları tehdit ediyorlar. Kısacası tüm masaüstü ve mobil cihazlar tehdit altında. Ancak fidye yazılımları ağırlık olarak Windows ve Android cihazları hedef alıyor.

Aynı zamanda cihazınıza bulaşması da çok kolay. Çok yaygın olarak, fidye yazılımları bilgisayara açılan şüpheli eklerleden, tıklanan şüpheli linklerden ve uygulama indirilen üçün parti mecralardan bulaşıyor. Ayrıca fidye yazılımları yasal internet sitelerine de bulaşabilirler: Güncel örnek olarak, siber suçlular fidye yazılımlarını kullanıcılara bulaştırmak için reklam ağlarını kullanıyorlar.

Diğer bir yandan, kullanıcılara önemli bir şey indirtip açtığını düşündürmek çok basit. Bankadan gelmiş bir mail ya da önemli bir program yüklemesi. Dosya açıldığı ya da program kurulduğunda, kullanıcı kendi bilgisayarına fidye yazılımı kurmuş oluyor.

Muhtemelen fidye yazılımları ile temel sorun, zararlı yazılımı silmeniz problemi çözmüyor. İyi bir anti virüs programı ve özellikle belli uygulamalar, genellikle fidye yazılımlarına karşı çok etkili çözüm sunuyorlar. Ama eğer zararlı yazılım dosyalarınızı şifrelerse, verilerinize erişebilmek için şifreyi açmanız gerekmektedir.

Dahası, fidye ödemek birkaç sebepten dolayı çok can sıkıcıdır. Öncelikle, fidye ödeyecek paranız olmayabilir. İki, fidye ödemek siber suçluları motive ederek bu işe devam etmelerini sağlar. Üçüncüsü ve en önemlisi, fidye ödedikten sonra sorununuzun çözüleceğine emin olamazsınız. Araştırmalarımıza göre fidye yazılımı. Ayrıca bir defa size zarar veren birine neden güvenip istediği parayı mağdurlarının %20'si fidye ödemesine rağmen dosyalarını kurtaramadı.

Zeroday Nedir ?

Zeroday Açıklıkları ve Çözümler

Sıfırıncı Gün Açıklıkları - Zeroday

Zeroday (Sıfırıncı gün açıklıkları) daha önceden bilinmeyen veya tespit edilmemiş ancak ciddi saldırılara yol açacak zafiyetler barındıran yazılım veya donanım kusurlarıdır. Zeroday açıklıkları çoğunlukla saldırı gerçekleşene kadar tespit edilmesi zor olan zafiyetlerdir.

Zeroday saldırısı ise geliştiricilerin bir yama veya düzeltme yayınlamaya fırsat bulamadan saldırganın zafiyeti istismar etmesi ve zararlı yazılımı yaymasıyla gerçekleşir. Bu nedenle bu zafiyet sıfırıncı gün açıklığı (zeroday) olarak isimlendirilmiştir.

Zeroday saldırısına neden olan etmenler:

- Yazılımcıların geliştirdikleri uygulamanın bir zafiyet barındırdığının farkında olmadan uygulamayı kullanıma geçirmeleri
- Saldırganın zafiyeti geliştiriciden önce saptaması veya geliştiricinin bir düzeltme üretmesine fırsat vermeden istismar etmesi
- Zafiyet hala istismar edilmeye açık ve ulaşılabilir iken saldırganın istismar kodunu yazıp uygulaması

Yama yazılıp kullanıma alındıktan sonra açıklık artık zeroday olarak adlandırılmaktan çıkmaktadır. Zeroday açıklıklarının tespit edilme süreci bazen aylar hatta yıllar almaktadır.

Zeroday Açıklıklarını Saptamak için Çözümler

Sandbox

Türkçede Kum havuzu olarak adlandırılan Sandbox sıkı kontrol ve izin mekanizmaları uygulanarak ayrık ve kısıtlı olarak dizayn edilmiş, programın üzerinde çalıştığı sisteme herhangi bir hasar vermeden veya zararlı yazılım bulaştırmadan denenebildiği ortamdır.

Sandbox içerisinde bir program çalıştırıldığında normal bir sistem üzerinde çalışıyormuş gibi işlevleri yerine getirir; ancak uygulamanın oluşturmak veya değiştirmek istediği herhangi bir şey program çalışmayı durdurduğunda kaybedilmektedir, yani saklanmamaktadır. Sandbox sistemler aynı zamanda belirli zararlı yazılım tehditlerini analiz etmek ve öğrenmek için de kullanılmaktadır. Zeroday saldırılarını denetleyip önleme için geliştirilmiş bazı

Sandbox ürünleri işlemci düzeyinde denetim yaparak atak vektörlerinin daha işlenmeye başlamadan sona erdirilmesini sağlamaktadır. İşletim sistemi düzeyinde denetleme sağlayan sandbox ürünleri ise dosya davranışlarını ve linkleri inceleyerek şüpheli aktiviteleri tespit etmeye çalışmaktadır.

Zeroday Açıklıklarını Tespit için Yöntemler

Bilgisayar sistemlerinin hemen hemen her platformda uygulama alanı bulması ile birlikte bilgi teknolojileri gün geçtikçe karmaşıklaşmakta ve bu nedenle siber saldırı olasılığı da artmaktadır. Birçok kurum IDS/IPS, güvenlik açığı tarama araçları, anti-malware ve antivirüs gibi imza-tabanlı güvenlik araçlarıyla bilinen tehditleri denetlemeye çalışmaktadır, ancak Zeroday gibi içerdeki bir yazılımcının yanlışlıkla zafiyetli olarak geliştirdiği bir uygulamanın arzettiği tehlike çoğu zaman bu geleneksel yöntemlerle tespit edilememektedir. Birçok kurum bu ilk elden gelebilecek tehdidi algılayıp yanıt verecek bir donanıma sahip değildir. Zeroday açıklıkların tespit edilip önlenmesi sürecinde sadece olay kayıtlarının değil işleyişin analizi de büyük öneme sahiptir. Uzmanlar Zeroday açıklıklarının saptanmasında en kullanışlı yöntemin sistemdeki anormal davranışların tanımlanıp yöneticilerin hızlı bir şekilde alarma geçirilmesini sağlayan davranış bazlı(behavior-based) analiz araçları olduğunu vurgulamaktadırlar. Davranış bazlı analiz araçlarında Hidden Markov Modeli ve istemci bir honeypot sistemi kullanılmaktadır.

Bazı ürünler ise Zeroday açıklığını tespit etmek için beyaz listede olmayan portlardan giden yetkisiz internet trafiği için kural oluşturmaktadır. Bir diğer yöntem ise alıcı IP adresi bilinmeyen tek bir kaynakla ile iletişim gibi bir etkileşim için alarm oluşturulmasıdır.

IPSec VPN (Internet Protocol Security – İnternet Protokolü Güvenliği)
IPSec, şifreleme ve güvenlik hizmetlerini kullanarak IP protokollerinin güvenlik ihtiyaçlarını karşılamak için IETF (Internet Engineering Task Force – İnternet Mühendisliği Görev Gücü) tarafından geliştirilmiş bir güvenlik protokolüdür. Bu protokol sayesinde veriler ağ üzerinde güvenli bir şekilde gitmesi gereken hedeflere ulaşır. IPSec ağ katmanında çalışarak IP paketlerinin IPSec aygıtları arasında korunmasını ve kimlik denetiminin gerçekleşmesini sağlar. IPSec ağ katmanında çalıştığı için uygulamadan bağımsız olarak her veriyi şifreler ve şifre sonrası oluşturduğu başlık ile verinin İnternette rahatlıkla yolculuk edebilmesini sağlar. Bu yüzden günümüzde VPN (Virtual Private Network - Sanal Özel Ağ) teknolojisinin altyapısını oluşturmaktadır. Genellikle IPsec ile VPN kavramları birbirleriyle karıştırılır. VPN iki uç nokta arasında bir sanal ağ kurmak için kullanılır. IPSec, oluşturulan VPN bağlantılarına güvenliği arttırıcı fonksiyonlar sağlar. VPN oluşturmak için katman 2 ve katman 3 de farklı yollar mevcuttur. IPSec bu yollardan sadece bir tanesidir. Günümüzde İnternet'in gelişmesiyle birlikte IPSec VPN bağlantılar kolaylıkla yapılabildiğinden bu iki kavram iç içe geçmiş durumdadır.
IPSec protokolleri ağ katmanında çalıştığı için diğer güvenlik protokollerine göre daha esnektir. SSL (Secure Socket Layer - Güvenli Soket Katmanı), TLS (Transport Layer Security - Geçiş Katmanı Güvenliği), SSH (Secure Shell - Güvenli Kabuk) 4. ve daha üst katmanlarda çalışmaktadır. IPSec, içinde TCP ve UDP'nin de bulunduğu katman 4 ve yukarı katman protokolleri koruyabilir. IPSec'in diğer güvenlik protokollerinden bir üstünlüğü ise IPSec'in uygulama katmanından yani kullanıcıların yazılımlarından bağımsız çalışabilmesidir. Fakat diğer protokolleri (SSL gibi) kullanabilmek için kullanıcının yazılımının o protokolü desteklemesi gerekmektedir.

IPSec çerçevesi 5 temel yapı bloğunu içerir.

- 1. blok IPSec protokolüdür. ESP ve AH seçeneklerini içerir.
- 2. blokta gerekli olan güvenlik ve gizlilik (confidentiality) derecesine göre kullanılacak olan şifreleme algoritmaları bulunur. (DES, 3DES, AES, SEAL)
- 3. blok MD5 veya SHA kullanarak gerçekleştirilecek bütünlüğü (integrity) içerir.
- 4. blok içeriğin ne kadar paylaşılacağını gösteren PSK ve RSA gibi kimlik doğrulama denetimlerini bulundurur.
- Son blok Diffie-Hellman algoritmalarını içerir. Gerekli özel ihtiyaçlara göre 4 farklı DH algoritmasından herhangi biri seçilebilir.
  IPSec ağ geçitleri arasında, istemciler arasında ve ağ geçitleriyle istemciler arasında güvenli veri aktarımını sağlayabilir. IPSec çerçevesi kullanılarak 4 temel güvenlik gereksinimi gerçekleştirilebilir.

Gizlilik (Confidentiality)

IPSec şifreleme metotlarını kullanarak gizliliği temin eder. Güvenliğin derecesi şifreleme algoritmasında kullanılan anahtarın uzunluğuna bağlıdır. Anahtar ne kadar kısa olursa, şifreyi kırmak o kadar kolay olur ve güvenlik açığı oluşur. Örnek olarak 64 bitlik bir anahtarın bilgisayar tarafından kırılması yaklaşık olarak 1 sene sürebilir.

- Des – 56 bit uzunluğunda simetrik kriptolama tekniği kullanan bir sistemdir. Aynı anahtarla şifrelenen veri gene aynı anahtarla açılabiliyorsa simetrik bir şifreleme algoritması kullanılıyor demektir.

- 3Des – Des'in farklı bir çeşididir. 3 tane birbirinden bağımsız 56 bitlik şifreleme kullanarak Des'e göre daha kuvvetli bir güvenlik sunar.
- Aes – 3Des ve Des'e göre daha güvenli bir sistemdir. 128 bit, 192 bit ve 256 bit olmak üzere üç farklı anahtar uzunluğuna sahip olabilir.
- Seal – 1993 yılında Philip Rogaway ve Don Coppersmith tarafından geliştirilmiş, 160 bit anahtar uzunluğunu kullanan bir sistemdir.

Bütünlük (Integrity)

IPSec veri bütünlüğü algoritmalarını kullanarak iletilecek bir verinin hedefe değişmeden sorunsuz bir şekilde ulaşmasını sağlar. HMAC (Hashed Message Authentication Codes - Şifrelenmiş Mesaj Doğrulama Kodu) sahip olduğu "hash" değeri yardımıyla verinin bütünlüğü koruyan bir algoritmadır. Amacı verinin kriptolanmasını sağlamak değil, verinin yolda değiştirilmesini önleyerek verinin doğruluğundan alıcı tarafın emin olmasını sağlamaktır. Gönderici tarafında veri şifrelenir ve Hash algoritmasından geçirilerek bir Hash değeri üretilir. Alıcı tarafında ise Hash algoritmasında tersten geçirilerek üretilen Hash değerinin gönderici tarafında elde edilen değerle aynı olup olmadığına bakılır. Değer aynıysa verinin bütünlüğü sağlanmıştır, farklıysa veri değişmiştir ve kullanılmaz.
İki çeşit HMAC algoritması vardır:

- HMAC – MD5 – 128 bitlik şifrelenmiş veriyi kullanır. Algoritmadan çıkmış hali gene 128 bitlik bir Hash değeridir.
- HMAC – SHA1 – 160 bit uzunluğunda anahtarlama tekniği kullanır. Bu algoritma güvenlik açısından HMAC – MD5'den daha güçlüdür.

Kimlik Denetimi (Authentication)

Genel olarak bir belgenin kimlik denetiminin sağlanması imzalama yöntemiyle olur. Elektronik cihazlarda ise sayısal imza adı verilen gönderen cihazın özel şifresini taşıyan paketler yardımıyla kimlik denetimi sağlanır. IPSec kimlik denetimini sağlamak için PSK ve RSA olmak üzere iki farklı algoritma kullanır.

PSK – Ön-paylaşımlı gizli anahtarlama metodu anlamına gelmektedir. Cihazlarda kimlik denetimini sağlamak için belirlenmiş olan bir sayısal değer elle gereken cihazlara girilir. Her cihaz karşısındaki cihazın değerini öğrendikten sonra ağ güvenli hale gelmiş olur ve veri aktarımı başlar. Girilen sayısal değer cihazın imzası olarak kabul edilmiş olur ve kimlik denetimi sağlanır.

RSA – Asimetrik bir şifreleme algoritmasıdır. Simetrik şifrelerdeki gibi tek anahtar kullanılmasının yerine biri gizli diğeri açık olmak üzere iki anahtar kullanır. Özellikle çok kullanıcısı olan sistemlerde oldukça geçerlidir. Sistemin güvenilirliği ve hızını etkileyen en önemli faktör kullanılan anahtarın uzunluğudur.
Kimlik denetimini sağlamak için diğer bir yöntem de IKE (Internet Key Exchange – İnternet Şifre Değişimi) adı verilen protokuldür. IKE kimlik denetimini, kullanıcı adı ve şifre, tek seferlik şifre, sayısal sertifikalar gibi çeşitli yöntemlerle gerçekleştirir.

Güvenli Anahtar Değişimi (Secure Key Exchange)

IPSec cihazlar arası açık anahtar değişimini sağlamak için Diffie-Helman adı verilen algoritmaları kullanır. Cihazlar arasındaki şifreleme ve şifreyi çözme işlemlerini gerçekleştirmek için en kolay yöntem anahtar değişimini sağlamaktır. Diffie-Helman, kısaca DH algoritmaları sayesinde güvenli olmayan bir kanal üzerinden veri aktarırken bile cihazlar

arasındaki anahtar değişimi sorunsuz bir şekilde gerçekleştirilebilir.
DH algoritmaları DH 1, DH 2, DH 5 ve DH 7 olmak üzere 4 farklı şekilde gruplanmıştır. Temelde bu algoritmalar arasındaki fark şifreleme yaparken kullanılan bit sayısıdır.

- DH 1 768 bit, DH 2 1024 bit, DH 5 1536 bitlik anahtar kullanır.
- CISCO 3000 serisi cihazları DH 1-2-5'i kullanırken, Des ve 3Des şifreleme metotları DH 1 ve 2'yi, AES metodu ise DH 2 ve 5'i kullanır.

IPSec Protokolleri

Daha önce şekilde de gösterildiği gibi IPSec protokolleri IPSec yapı bloğunda 1. sıradadır. AH ve ESP olmak üzere 2 çeşittir.

AH (Authentication Header – Kimlik Denetimi Başlığı)

AH protokolu genellikle gizlilik gerekli olmadığında ya da izin verilmediğinde kullanılır. İletim sırasında oluışabilecek değişiklikleri engellemek, gönderilen paketin bütünlüğünü korumak için IP paketine sıra numarası verilir. Eğer alıcı tarafına paketler sıra numarasına uymayacak şekilde ulaşırsa paketler kabul edilmez. Bununla birlikte AH gizlilik sağlamadığı için tek başına kullanılması durumunda güvenlik açığı oluşturabilir.

ESP (Encapsulating Security Payload – Kapsüllenen Güvenlik Yükü)

ESP protokolu gizilik ve kimlik denetimini beraber sağlayabilir. Bu protokol öncelikli olarak AH tarafından sıra numarası verilmiş IP paketlerini belirlenmiş algoritmalardan faydalanarak şifrelemek ve hedefe ulaştığında aynı algoritmaları kullanarak çözümlemektir. Böylece AH tarafından oluşabilecek güvenlik açığı engellenmiş olur.

AH ve ESP protokolleri IP paketlerine iki farklı şekilde uygulanabilir.

Transport Mode (Aktarma Modu)

Bu modda güvenlik sadece OSI katmanlarından Transport katmanı ve üzerinde sağlanan bir özelliktir. Transport modu IP paketinin AH veya ESP ile korunmasını sağlar. Paketin yük bölümü üzerinden koruma gerçekleşirken, gerçek IP adresinde değişiklik meydana gelmez. Aynı yerel ağ içerisinde bulunan cihazlar tarafından kullanılabilir.

Tunnel Mode (Tünel modu)

Bu modda güvenlik bütün IP paketi üzerinden gerçekleştirilir. Gerçek IP paketi şifrelenir ve başka bir IP paketi yardımıya kapsülleme yapılır. Genel olarak tünel modu veriler farklı bir ağdan geçiş yapacağı zaman kullanılır. Tünel modunda şifreleme işlemi veriler ağdan çıkış yaparken ağ geçidi (gateway) üzerinde yapılır. İç ağlarda IPSec kullanmaya gerek yoktur.

Sonuç olarak IPSec veriyi, kriptolayan (encryption), bütünlüğünü sağlayan (integrity) , kimlik doğrulaması (authentication) ve verinin network üzerinde güvenli iletimini (Secure transmission) sağlayan bir ağ standartıdır.

Kaynaklar :

1- https://wmaraci.com/nedir/rootkit
2- https://www.kaspersky.com.tr/blog/ransomware-for-dummies/2713/
3- https://www.beyaz.net/tr/guvenlik/makaleler/zeroday_nedir.html
4-https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ipsec-vpn-(internet-protocol-security-internet-protokol%C3%BC-g%C3%BCvenli%C4%9Fi)