Distributed Denial of Service

DDoS

Önsöz

Bu makale DDoS saldırılarını ve korunma yöntemlerini konu almaktadır.
Yalın bir dil kullanarak prensiplerini dile getirmeye çalıştım.

Hedef kitlem bilgisayar kullanıcıları ve “deneyimsiz” sistem yöneticileri olduğu için konunun derinlemesine inmedim. Buna rağmen sorunun anlaşılabilir bir dil ile çerçevesini çizmiş olduğumu umuyorum.

Önder Gürbüz

Kurumsal bir kimliğe sahipseniz

Zamanında, yani saldırıya uğramadan önce…

- ✓ Bilişim teknolojisinde deneyimli elemanlarınızdan, kurumunuzda mevcut bir bilişim teknolojisi güvenlik görevlisi varsa veya kurum dışı bu konuda profesyonel destek alarak gerektiğinde süratle bir araya gelebilecek bir ekip oluşturun. Bu acil müdahale ekibinin gerekli tüm teknik ve bu gibi durumlarda anlanması gereken ek çalışmaları yapabilmesi için gerekli maddi / manevi desteği oluşturun.
- ✓ Gecikmeksizin kurumunuzun ilgili yönetim kurulu veya yöneticisini durumdan haberdar edin.
- ✓ Durumu kendi Internet Service Sağlayıcısına bildirip birlikte ne gibi önlemler alabileceğinizi irdeleyin.
- ✓ Durumu hukuk danışmanınıza veya Avukatınıza bildirerek suç duyurusunda bulunun.
- ✓ Halkla ilişkiler uzmanlarınızın bu gibi durumlara hazırlıklı olmasını ve gerektiğinde acil olarak medyaya duyuru yapabilecek şekilde gerekli dokümanların hazırlanmış olduğunu denetleyin.
- ✓ Müşteri ve beraber çalıştığınız şirketleri potansiyel saldırıdan haberdar edin.
- ✓ Bilirkişi vasıtasıyla DDoS Migration Appliances üzerine fikir edinin ve kendi güvenlik ihtiyacınıza göre uygulamaya koyun.
- ✓ Sistem arasına yerleştirilen Honeypot'da, ileriye yönelik, bu konuda oldukça yardımcı olabilir.
- ✓ Internet Servis Sağlayıcısının DDoS Migration Services imkânlarından faydalanın.

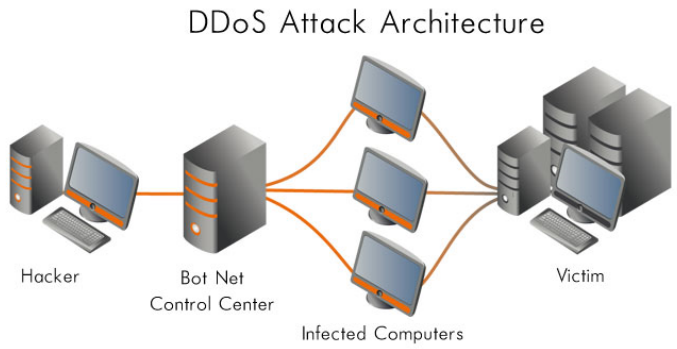
- ❖ Kullanılan Firewall 'ün kendisi de (bottleneck of DDoS attacke) bir sorun teşkil edebileceği için zamanında denetlenmesinde fayda var.

Eğitim sürecini dâhil etmeden 27 senelik mesleğim olduğu için ve bilgi birikimine – akademik derecede – çok güvendiğim Black-Hat Hackerlerden edindiğim bilgiye göre Alman Web-hoster'ler (hepsi değil tabii, beli başlı bir kaç tane var ve bu konuda çok ileri derecede güvenlik sunuyorlar. Reklam yapmamak namına isim vermek istemiyorum. Benimle irtibata geçildiğinde – ücretsiz – yardımcı olmaya çalışırım) en zor hacklanabilen siteleri oluşturuyor. Kaldı ki ilgili kanunlarıyla dünya çapında Almanya bu konuda en ön sıralarda yer almaktadır. Özellikle kişisel bilgilerin korunması konusunda! Unutulmamalıdır ki servis sağlayıcıların büyük bir bölümü Amerika Birleşik Devletlerinde ve İngiltere / İrlanda'da bulunmaktadır. Bu ülkelerin de bu konuda ne kadar güvenilir olduğu sanırım hepimizin malumudur. Internet küresel bir olgu olarak karşımıza çıksa da, Web sunucuları bulunduğu ülkelerin ilgili kanunlarına tabidir. Özellikle ABD bu konuda çok tehlikelidir. Ulusal güvenlik kanunu bu konuda bütün kapıları açabilecek genişliktedir! Bu uyarının dikkate alınacağını umuyorum.

En çok uygulanan 6 siber saldırı yöntemi

- ✓ Hedef gözetilerek ve zararlı yazılım (mesela casus) yerleştirmek amaçlı belirlenen Web sunucusu veya sitenin hacklanması. Bu saldırıların bir hedefi de veri tabanları olabiliyor.
- ✓ Drive by Exploits veya Drive by Download (iki tabirde kullanımda) İnternette salt bir sayfayı açmanızla (exploits) veya bir siteden bir resim, video, pdf, müzik, çalıştırılabilir herhangi bir yazılım veya dokümanla – kısacası herhangi bir download'la– kendi bilgisayarınızın zararlı bir yazılım sayesinde bir nevi "saatli bombaya" dönüşmesi. Uzaktan kumanda vasıtasıyla saldırı anında bilgisayarınız yüzlerce, (yüz)binlerce bilgisayardan oluşan bir ağının parçası olarak >>> sizin bilginiz dışında <<< suç aletine dönüşmesi.
- ✓ Şeklen farklı ancak aynı hedefe yönelik eMail (Maleware) veya genelde sosyal ağlarda uygulamaya konan sosyal mühendislik ile kullanıcının bilgisayarı saldırgan tarafından hâkimiyeti altına alınması. Bakın burası çok önemli, özellikle deneyimsiz kullanıcılar >>> düşünmeden, alelacele <<< bir tıkla zombie'ye dönüşür! Bu bakımdan kurumunuzda çalıştırdığınız elmaların bu yönde eğitilerek uyarılması gerekir. Security Through Education!
- ✓ Distributed Denial of Service (DDoS) ikinci ve üçüncü yöntem ile ele geçirilen bilgisayarların (zombie) belirlenen hedefe eşzamanlı yönlendirilmesidir.
- ✓ Spam veya Drive by Exploits vasıtasıyla gelişigüzel "dağıtılan" kimlik bilgileri toplamaya yönelik saldırı şekli.
- ✓ Kademeli saldırı. Merkezi güvenlik altyapısı (örneğin TLS/SSL) çökertildikten sonra asıl hedefe yönelme.

DDoS saldırılarını önlemek için alınabilecek önlemler



- ✓ Hangi işletim sistemini kullandığınıza bağlı olarak Webserverler için DDoS saldırılarında ulaşımı iyileştiren modüller vardır. Bunları kullanın.
- ✓ IP başına bağlantı imkânlarını sınırlayınız veya bir IP'den gelen sorgulamayı gecikmeli olarak yanıtlatın.

- ✓ TCP-SYN Cookileri çalıştırın.
- ✓ Webserver girişini Port 80 ve 443 (TLS/SSL) ile sınırlayın.
- ✓ Saldırıya uğradığınızda hazırlamış olduğum GeoISPIP dokümanı yardımıyla da IP filtrelerini çalıştırın. Örneğin saldırı Almanya'dan geldiğini gördüğünüzde Almanya ya ait IP numaralarını saldırı süresince filtreleyin. Bu zaman zarfında Almanya'dan gelen tüm, yani yasal sorgulamalar dâhil önlenir (Blackholing). GeoISPIP
- ✓ Gerekli görüldüğünde, daha büyük hasarları önlemek namına, geçici bir süre için saldırıya uğrayan IP numarası veya URL adreslerini Router üzerinden iptal edin (Sinkholing).
- ✓ Diğer filtreleme önlemleri mesela http temelinde düzenlenen saldırılarda Http-Header üzerinden önemli bulgulara rastlayabilirsiniz. Tabii bu işlemi yapabilmek için belli bir bilgi birikimine sahip elemanlara ihtiyacınız olacaktır.

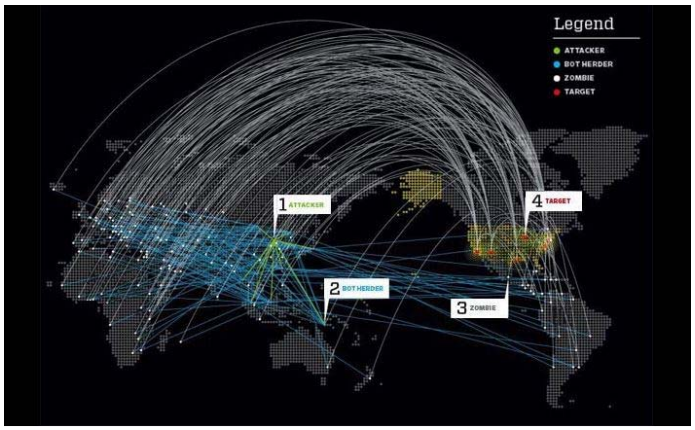
Yardımcı olabilecek ek önlemler

- ✓ Monitoring mesela Microsoft Network Monitor ile.
- ✓ Ve tabii bu işin olmazsa olmazı…
  İletişim protokolleri! Birçok sistem yöneticisi sistemi yavaşlatıyor gerekçesiyle protokolleri çalıştırmazlar. Ancak protokoller bu gibi durumlarda olağanüstü yardımcı bilgiler sunarlar.
- ✓ Web sitelerinizin öncellikli olarak HTML üzerinden hazırlanmasına özen gösterin. Hackerin saldırı alanını önemli ölçüde kısıtlamış oluyorsunuz.

Not: Etik olarak benim gibilerin hackerlerle ilgisi olabilir mi?
Evet, olabilir! Bu işlerin eskileri, bu gibi olayları bir nevi bilgi alışverişi olarak görürler. Bilgi yarışması gibi bir şey. Zihin sporu, al gülüm – ver gülüm misali. Tabii iki tarafta bu saldırıların ardında milyar dolarlık bir sanayinin "gizlendiğinin" bilincinde olarak, bilgi alışverişinin püf noktalarını bir yere kadar gizlerler ☺

Bot-Net

Bazı Bilişimciler saldırı yöntemlerini eski ve yeni diye ikiye ayırma eğilimindedir. Tecrübelerime dayanarak diyebilirim ki eski ve yeni yoktur!
Günümüzde “her iki yöntemde” kurumların donanımına, bilgi düzeyine ve maddi imkânlarına bağlı olarak ne yazık ki başarıya ulaşabilmektedir.
DDoS saldırılarının bir ayağını Bot-Net’ler oluşturur. Bot-Net aslında bir yazılım olup yukarıda tarif edilen yöntemlerle yayılması sağlanır.



Bot-Netler, Spam-Mail, Keylogging, Phishing, ticari casusluk, korsan yazılım satmak ve yayınlamak (File-Sharing) için de kullanılmaktadır.

Bot-Net şematiği

- ✓ Bot-Master (Bot-Herder) bir yazılım sayesinde, bilgisayarların güvenlik zaaflarından yararlanmak suretiyle veya sosyal ağlar sayesinde, internet üzerinden kurbanlarını bulur.
- ✓ Zombie haline dönüşen bilgisayarlar Command and Conrtol (CC) yani Bot-Master ile baglantı kurar.
- ✓ Bot-Master zombilerin veri tabanını güncelleyerek gerekli komutları verir.
- ✓ Bot önceden belirlenen IP adreslerinde yeni kurbanlar aramak için işe koyulur.
- ✓ Böylelikle Bot’a yeni katılan zombieler CC’ye bağlanarak kendilerini güncellerler.

“Eskiden” sistemlerin güvenlik açıkları kullanılırken (Port 139, 445, 135, 1025, 80, 135, 2745 gibi) günümüzde Social Engineering, File-Sharing (Peer to Peer ağları), Instant Messaging, eMail eklentileri ve sitelere yerleştirilen kodlar sayesinde (Drive by Download, Drive by Infection) yöntemleri kullanılmaktadır.

Son söz

Verdiğim örneklerden anlaşılacağı gibi hepimizin, her gün…

Düşünmeden, irdelemeden ve sorgulamadan (!)

“Otomatik” yaptığımız işlemlerin her yıl devletlerin, şirketlerin ve en sonunda her birimizin maddi ve manevi zararına olduğunu göstermektedir. Bu yönden bakıldığında…
Düşünmeden, alelacele bir tek tıklama…
Milyon hata milyarlarca zarar verebilir. Önce aklımızı sonra bilgisayarımızı kullanalım.

Saygılarımla

Önder Gürbüz
2013
Almanya

www.gurbuz.net