DDOS v2

Program Ejder tarafindan, SaVSaK.CoM icin yazilmistir. Tum haklari Ejder e aittir. Programin kullanmindan dolayi gelecek zararlarin hic biri Ejder ve Savsak.com ‘u ilgilendirmez.

Program icindeki bolumler;

- DDos
- Site Sawsaklama
- Snifer
- Searcher

4 ana bolumden olusmaktadir program. Her bolumun alt alanlarida bulunmaktadir. Bunlardan ve ozelliklerinden kisaca bahsedecegim. Ilgili konu ve kisimlarla ilgili daha detayli bilgiyi program icersindeki “?” yani help kisimlarindan ogrenebilirsiniz.

1- DDos

8 cesit saldiri modeline sahiptir. Bunlar kullanim yerleri ve ozelliklerine gore birbirlerinden farklilik gostermektedir.

- HTTP Saldirisi (en gelismisi)

En gelismis saldiri modelimizdir. Her turlu site icin gecerlidir. Istege bagli cookie, referans, path ekleme ozelliklerine sahiptir. En onemli ozelligi 60+ a yakin farkli istekde bulunabilmesidir. Icersinde 14 cesit browser tanimi ve bir o kadarda encoding, dil, path, referans sayilari ile cesitlenmektedir. Burdaki amac sabit bir saldiri degil, kendimizi bir network cikisi olarak gosterip, saldirinin etkisini arttirmaktir. Tek cesit paket yerine, cok cesitli farkli kisilerden, pclerden geliyormus izlenimi verip , saldiri boyutunu buyutulmektedir.Cok etkili bir saldiriya sahiptir. Ozelliklerindeki Cookie degeri? Bize uyelikli sistemleri gecmemiz, o tur sitelerin ic kisimlarinada saldirinin mumkun olmasini saglamaktadir. Cookie bildiginiz gibi tanimlayici bilgidir. Saldiri yapacagini site nin , kritik sayfalarinin yollarini path (yol) kismina ekliyerekden, saldirinin etkisi arttirilabilir. Unutmayinki database islemlerinin en cok islenen , yapilan kisimlarina saldirilar , sitenin cokusunu hizlandiracaktir.

Site/IP : bu kisma , sitenin Domain adini yazmaniz gerek. Su sekilde -> www.siteadi.com gibi. Sakin site URLsi, full yazmayin. Saldiracagimiz sayfalari baska yerden eklicez. Burda saldirilacak domain yazilmali.

Port: bu kisim genelde 80 dir. Ama bazi guvenlik nedeniyle, farkli port lardan http servisi veren , guvenlik , ticari siteler icin degistirilebilir yaptim.

Cookie: Eger sitede saldiracaginiz kisimlar, uyelik girisi gerektiriyorsa eger, o zaman Sniferr, site sawsaklama yada baska bir programla siteye giris yapip, size yazilan cookie degerlerini bu kisma yapistirmaniz gerekecektir. Bu kisma sadece

cookie degerini yazmalisiniz mesela -> admin=1&user:Ejder&hash=ABRE3407A739 seklinde ..

Yol: Bu kisim bizim saldircagimiz sayfalari icermektedir. Domainden itibaran hangi dizinde ise o kisimlari yazmaniz gerekecek. Mesela saldircagimiz yer http://www.savsak.com/news.asp ise , o zaman sadece -> news.asp yazip eklemelisiniz. www.savsak.com/forum/memberlist.asp?get=all gibi bir yere saldircaksaniz, o zaman -> forum/memberlist.asp?get=all seklinde yazip eklemeniz gerek. Saldircaginiz sayfa sayisini ne kadar arttirrirsaniz o kadar etkili olur. Ayrica saldircaginiz sayfalarin , Veritabani islemlerinin en cok yapildigi yerlere yapmaniz , saldiri etkisini arttirmaktadir.

Referans: Bu kisim saldirinin hangi siteden geldigini bize gosterecektir. Kimi siteler bu ozelligi LOG lar, bizde saldirinin yerini ve turunu, capini, etkisini arttirmak ve gizemimizi korumak icin, bu kisma site isimleri eklemeniz yeterlidir. Mesela ; http://www.google.com/arama.asp ekledigimizde. bu site ve sayfa uzerinden referans gitmis olacak. Yani saldirilan yer, boyle gorecektir ☺ bu kismi daha garip site yada saldirdgimiz yerin kendi site uzantilarini yazadigimiz taktirde, olusacak manzara? Saldirdigimiz yer , kendi kendine saldirmis gibi izlenim verecektir. DDOS oldugu anlasilmasi guc olacak ve cokus hizlanacaktir.

Ornek; saldiracagimiz yer -> http://www.savsak.com/uye.asp , http://www.savsak.com/forum/default.asp, http://www.savsak.com/new.asp, http://www.savsak.com/news.asp?id=66 gibi 4 sayfa uzerinde odaklanacaz. O zaman su sonuclar cikiyor.

Domain : www.savsak.com

Cookie: uyelik istemedi ici bos birakacaz.. isteseydi, cookie degerimizi yapistircaktik.

Yol: uye.asp, forum/default.asp, news.asp, news.asp?id=66

Referans : http://www.savsak.com/news.asp , http://www.google.com, http://www.carcurthackteam.com/ .... seklinde ekliyelim. Eger birine camur atacaksak? O sitenin adini kesin yazin ☺ o oyle boyle saldirdigimiz yer tarafindan farkedilcek. Birbirlerine dusurebiliriz ;)

- Veri Saldirisi

Site yada IP ye veri gondermemiz icindir. Eger siteye veri saldiri yapcaksaniz, bu POST yada GET ise, o paketi komple yazmaniz gerekecektir. Bu kisim sadece belirttiginiz Site yada IP ye, istediginiz Port dan, veri gondermeye yarar. Veri icergiini komple siz belirliyorsunuz. Bununla post ve get saldirilarinida gerceklestirebilirsiniz. Cok kullanisli bir ozelliktir bu. Eger bir bilgisayara veri gondereceksenis, IP adresini , portunu ve gonderilcek veriyi yazmaniz yeterlidir. Gonderilcek veri hex ise? Hex e cevirip veri kismina yazil gondermeniz gerekecektir. Bu kisim ile exploitleri cok guzel taklit edebilirsiniz.

- Normal

Bu ile digerlerini birbirlerinden ayiran ozellik ? saldiri icin kullanilan mimaridir. HttpDdos saldirisinda, socket yazilimi kullanilmaktadir. Surekli socket yaratip, karsiliksiz kapamaktaydi. Simdi bu seferki mimaride, webrequest yapisini

kullanilmaktadir. Bu digerlerine oranla biraz yavas kalabilir. Bunda sitenin kodlari komple cekiliyor. Kisacasi kaynak kod somuruyor. Bu saldiri seklide , coklu saldirilar icin etkili olacaktir. Bu saldiri mimarisine bazi ozellikler ekliyerekden, protected Url saldirisi ve proxy saldirisi gerceklestirilmektedir. Bu saldirida sadece sitenin domain adini yazmaniz yeterlidir. Direk URL yazmaniz yeterlidir. Mesela : http://www.savsak.com/news.asp

- Protected URL (Korumali siteler icin)

Bazi siteler, Protected URL yani sifre korumali giris ozelligini aktif etmektedir. O tur sitelere saldirmak icin, gelistirdim bu yapiyi. Zaten sitelere giris icin gerekli sifre ve kadi verilmektedir. Tek yapmamiz gereken, saldiracagimiz site Full url yazip, kadi ve sifre kisimlarini doldurup saldiriyi baslatmamizdir. Mesela : http://www.savsak.com/news.asp. Ne kadar cok kisi ile saldirirsak o kadar etkili ve hizli cokme yasaniz sitede.

- Proxyli

Proxyli Saldiri modelimizde, Ip mizi bir nevi korumak istenmistir. Bu kisim icin sadece saldircagimiz site URL si yazmamiz yeterlidir. Mesela : http://www.savsak.com/news.asp . Birde proxy listemizi eklememiz gerekir. Onuda ProxyKontrol kismindan ekliyoruz. O kisim icin ya internetten ceker, yada kendi localinizdekini yuklersiniz. Isterseniz check ettirirsiniz o size kalmis. Saldiri icin Calisan Proxyler kisminda proxy adresinin olmasidir.

- RPCNUKE v2 Saldirisi - Win2000/XP

RPCNUKE exploit inin donusturulmus halidir. IP adresine saldiri mumkundur. Cok agir calismaktadir. Eger gerekli sartlar saglandi ise, saldiri 1-2 gonderim ile makina halt olabilmektedir.

- Windows NAT Helper DDOS - XP SP2

Windows NAT Helper exploitinin donusturulmus halidir. IP adresine saldiri mumkundur. Cok agir calismaktadir. Eger gerekli sartlar saglandi ise, saldiri baslamasi ile, makinanin yavaslamasi ve halt olmasi ile sonuclanmaktadir.

- MSSQL 7.0 DDOS sp0 - sp1 - sp2 - sp3

MSSQL 7.0 exploitinin donusturulmus halidir. IP adresine saldiri mumkundur. Cok agir calismaktadir. Eger gerekli sartlar saglandi ise, saldiri baslamasi ile, makinanin yavaslamasi ve halt olmasi ile sonuclanmaktadir.

- Proxy Kontrol

Ister internet sitesinden guncel, isterseniz kendi bilgisayarinizdaki proxy listesini, yukleyebilir, kontrol ettirebilirsiniz. Bu kisim ayrica Prrox saldirisi icin kullanilmakatadirda.

- Uzakdan Yonet

Bu kismi ben Server lara yukledigimiz ufak shellciklerin kontrol edilip, toplu saldiri yapilmasi icin gelistirilmistir. Mesela Php, aspx de yazildigimi shelleri , hacklediginiz server lara yukledikden sonra, onlari uzakdan bu programla listeye ekliyerekden, DDOS yapmaniz mumkundur. Gonderdigi parametreler sabittir. O yuzden , gelen parametrelere gore, sizde kendi Shellini, ddos yaziliminizi yazabilirsiniz ve bu programla yonetebilirsiniz..

Kullanimia gelirsek, server lara yukledigiginiz shell adresilerini eklemeniz gerek listeye. Mesela; http://www.savsak.com/ejder.php gibi , eklemeniz gerek. Sonra Site/IP kismina , saldircaginiz DOMAIN i yazmaniz gerek, www.saldirilcaksite.com gibi. Port kismina -> 80 olmali. Dongu sayisi, shell kendi icinde kac kez donmesi gerektigidir. Saldirdiginizda, listedeki shellere, sira ile veri gonderip, saldirmalarini gerceklestirmektedir.

2- Site Sawsaklama

Genel olarak; POST ve GET saldirisi yapmak icin gerceklestirildi. 3 kisimdan olusmaktadir.

- **Post/Get Saldirisi**

Bu kisimda, POST ve GET saldirisinin yapildigi, parametrelerin ayarlandigi, saldiri taktiginin belirlendigi kisimdir. 2 sekilde bu kismi kullanabiliriz. Kolay olani Site Sihirbazi bolumunu secip, otomatik ayarlanmasini sagliyarak ; yada kendimiz manuel elimizle doldurarak.

Post/Get Adres: bu kisma saldirilacak sitenin get yada post edilcek adress yazilir. Mesela ; http://www.savsak.com/uyekaydet.asp gibi.. Eger Site Sihirbazi ozelligini kullanirsaniz, otomatik kendisi dolduracaktir.

Parametre Paneli: Bu kisma istediginiz isim ve degeri ekliyebilirsiniz. Get saldirilar icin , saldirilacak sitenin sonuna eklenir. Mesela; http://www.savsak.com/ekle.asp ise saldirilcak yer, Saldiri modelimiz GET ise, o zaman http://www.savsak.com/ekle.asp?isim=deger&isim2=deger2.. Seklinde kac tane parametre varsa yazilir. Eger Post saldiri modeli secildi ise, http://www.savsak.com/ekle.asp kismina o parametreleri post edecektir. Bunun bilincinde olmaniz gerekir.

Cookie: Eger uyelik sistemi ve cookie kontrollu erisimlerde bu kisma cookie degerini yazmaniz gerekir. Manuel yapiyorsaniz, ham cookie degerini yazmaniz gerekecektir. Eger Site Sihirbazi kullaniyorsaniz, otomatik oldurulcaktir.

Ayarlar: Post ve Get saldiri modelini seciyoruz. Eger site Sihirbazi ozelligini kullanirsaniz, otomatik secilcektir o ☺ . Burda onemli ikinci bir konu ise, Http Baslik ayar kismidir. Bu kisimda sabit bir mimari kullanabilirsiniz. Neden gerek duyduk derseniz? Benim saldiri modelim, random paketler gondermektedir. Saldirinin etkisini arttirmak icin. Fakat kimi siteler sabit paketleri kabul ediyor. O zaman Sabit paketler

gonderilmesi gerekecektir. O yuzden, 1 kereligine POSt yada get paketini yakalayip, o kisma yapistirmaniz yada site sihirbazi kulanip, aktif etmeniz gerekecektir. O zaman parametreler haric, hersey sabit olacak ve site %100 sasmaksizin kabul edecektir her veriyi ;). Bu kisim gozlem ve denemeler sonucu ortaya cikti.

Sozluk Ayari: Parametre kisminda eger Liste secimi yaparsaniz , o zaman bu kismi yuklemeniz gerekecektir. O kisimda, user ve sifre listesini yuklemeniz gerek. Eger amacimiz Sozluk saldirisi yapip uyelik sistemine saldirmak ise, o zaman saldirimi modunu secip, gerekli yeri doldurmaniz gerekmektedir. Bu kismi , kontrollu parametre gondermek ve Sozluk saldirisi yaparakdan, uyelik sitemini kirmaktir.

- **Site Sihirbazi**

Bu kisim , Site Sawsaklama yaziliminin en onemli yeridir. Kullanmasini iyi bilirseniz, cok kolaylikla Saldiri kismini sorunsuz halletmis olursunuz. Simdi tek yapmaniz gereken Site/URL kismina site adresini yazmak. Sonra saldircaginiz yer POST saldirisi ise, neresi ise o kisimdaki formu doldurup 1 kez post yapmaniz gerek. O otomatik tespit edecektir. Tespit ettiginde Saldiri kismina gidip gorebilirsiniz ne tur paremetre, cookie degerleri yakaladigini. Simdi burda dikkat etmeniz gereken yer, Aktif et olayidir. Gezerken POST saldirisi yakaliyacaksaniz, POST aktif, eger Get ise GET i aktif etmeniz gerek. Yada her ne olursa olsun ise ☺ o zaman ikisini secin. Zaten yakalandiginda bisiler, Saldirilar kismindan gozlersiniz. Bu yazilim ile zaten Ddos u gerceklstirmis oluyoruz bir nevi.

Key izleme; 1 kez deneme yaptiniz, post tespit edildi dendi, fakat saldiri kisminda parametre yok ? o zaman bu kismi aktif edecez. Cunku siteden gelen paremetreler 1 den fazla paket halinde gelmektedir. O yuzden onlari yakalmamiz icin, POST edilen degerlerden sadece birini bu kisma yazmaniz gerek. Onuda Sitenin kaynak kodundan, form icindeki “name” lerden birini secerekden yapabilirsiniz. Boylece tum paketler yakalanmis, saldiri icin gerekli parametreler sorunsuz yakalanacaktir.

- **Site Bilgisi**

Bu kisimda, Site sihirbazi ile gezdiginiz yerlerin, domain, link, cookie, kaynak kod bilgisini alabileceginiz kisimdir. Otomatik kendi kendini guncellemektedir.

3- Sniffer

Her turlu filtrelemenin yapilabilinecegi, kullanisli bir Sniffer yazilimidir. Gelen, giden tum paketleri yakalayabilir, izleyebilir, logluyabilirsiniz. 2 tur cikti verir; char ve hex olarak. Digerlerinden ayiran ozelligi, bilgisayarinizda sorunsuz calismasi, hizli, anlik yakalamasi, kolayca yonetilip, izlenebilmesi ve log tutma ozelligidir.

4- Searcher

Google, yahoo uzerinden arama yapan ve rfi aramasi yapan bolumdur. 2 kisimdan olusur.

- **Arastirmaci**

Google ve Yahoo uzerinden sorunsuz arama yapabilmektedir. 7 cesit ture sahiptir. Tek yapmaniz gereken aranacak kelimeyi yazmaniz ve turu secmenizdir. O size tum bulduklarini listeliyecektir.

Bu tur bir yazilim, site aciklarini arama ve bize liste halinde sunmasi istendiginde, cok buyuk katkisi olacaktir.

Ornek; Sql icin acik ariyacagiz. Aranacak kismina ; news.asp?id= yazmaniz yeterlidir. Arama tarzi: inurl: olmalidir. Bu yapiyi google ve yahoo da desteklemektedir.

- **Gelismis Rfi Arama**

Php inclusion acigini bulmak icin, tarama yapmak icin gelistirilmidtir. Rfi aramasi icin, once ayar cekmeliyiz.

Site Listesi: Burdan taranacak sitelerimizin listesini eklememiz gerekmektedir. 1 yada coklu site imkani sunulmaktadir.

Rfi Listesi: Otomatik program icindeki 622 cesit rfi eklenmetedir listeye. Siz isterseniz listeyi siler, yenisini eklersiniz yada uzerine ilave edersiniz. Bu liste , sitelerde taranacak kisimlardir. Php inclusion potansiyeli olan yerlerdir.

Shell Ayarlari: Bu kisim tarama yapilirken, acigin bulunmasi icin gerekli shell adresi ve tanimlayici bilgi degerini icermektedir. Shell adresini ordaki gibi sonunda ? isareti ile bitecek sekilde, kendi yada baska bir siteye yukleyip, adresini yazmaniz gerekir. Ben savsak.com icindeki shell adresini imha ettim. Ordaki sadece ornektir. Kendi shellinizi yuklemeniz gerekecek. Filtrelenecek kelime ise , Shell icinde yazmasi gereken kelimedir. Essiz olmasi gerek. Robot sayisida, kacarli arama yapilmasi gerektigidir. Ayni anda tarama sayisidir. Baglanti hiziniza gore ayarlayiniz. Ortlama 40 -50 olmasi yeterlidir. Demekki ayni anda 50 tane test yapacak ☺.

Shell in olusturulmasi; bos bir txt dosya acin. Icine <? echo "EjderWasHERE" ?> bunu yazin sadece. Sonra adini shell.txt yapin. Size kalmis bu kisimlar. Shell.txt yi sitelerden birine yukleyin ve adresini Shell adresi kismina yazip, sonuna '?' isareti koyunuz. -> http://www.savsak.com/shell.txt? Seklinde olacak. Filtrelenecek kelime kisminada EjderWasHERE yazmaniz gerek. Txt icinde yazdiginiz kelime olacak kisacasi. Shell ayar kismi bu kadar.

Yazilimin saldiri gucu, ozellikleri, saldiri taktikleri ; Ejder in bilgi birikimi, arastirmalari ve denemeleri sonucuna dayanarakdan tasarlanmis ve kodlanmistir. Yazilimdan gelecek her turlu zarar , sorun Ejder ve Savsak.com u ilgilendirmez. O yuzden kullanirken dikkatli kullanin. Program, HackTools potansiyelinde bir yazilimdir. Antivirus programlari uyari verebilir bu konuda. Bunun bilincinde olmanizda gerekmektedir.

Yazilim ilk kez acildiginda, savsak.com uzerinden 1 kereye mahsus, activation key isticektir. Eger savsak.com kapali ise, programla birlikde size verilen aktivasyon kodu ile programi acabilirsiniz.

Yazilim aktivasyon disinda, birde programin guncel yamasi, update yada yeni surum bilgisi icin kontrol etmektedir. Eger herhangi bir yenilik, duzenleme durumunda size bilgi verecek ve hic bir islem yapmicaktir. Yeni bir surum ciktiginda, savsak.com uzerinden tekrar indirmeniz, kurmaniz gekecektir.

Yazilimin her noktasini test etmeye calistim. Eger hata ile karsilasirsaniz , yada calismayan bir kismi ki? Her kismi denedim, calismaktadir. O zaman Ejder e iletirseniz , iletiniz incelenip duzeltilecektir. Programda suda olsun, bu ozelligi daha da gelistirsek gibi oneri ve somut bilgileriniz varsa, Ejder e iletirseniz programin sonraki surumlerinde katkida bulunmus olursunuz.

Irtibat adresim : ejder@savsak.com (sadece mail ile irtibat kurunuz)

Program Ejder tarafindan SaVSaK.CoM icin yazilmistir.
WwW.SaVSaK.CoM
by EJDER ;)

13 Kasim 2007