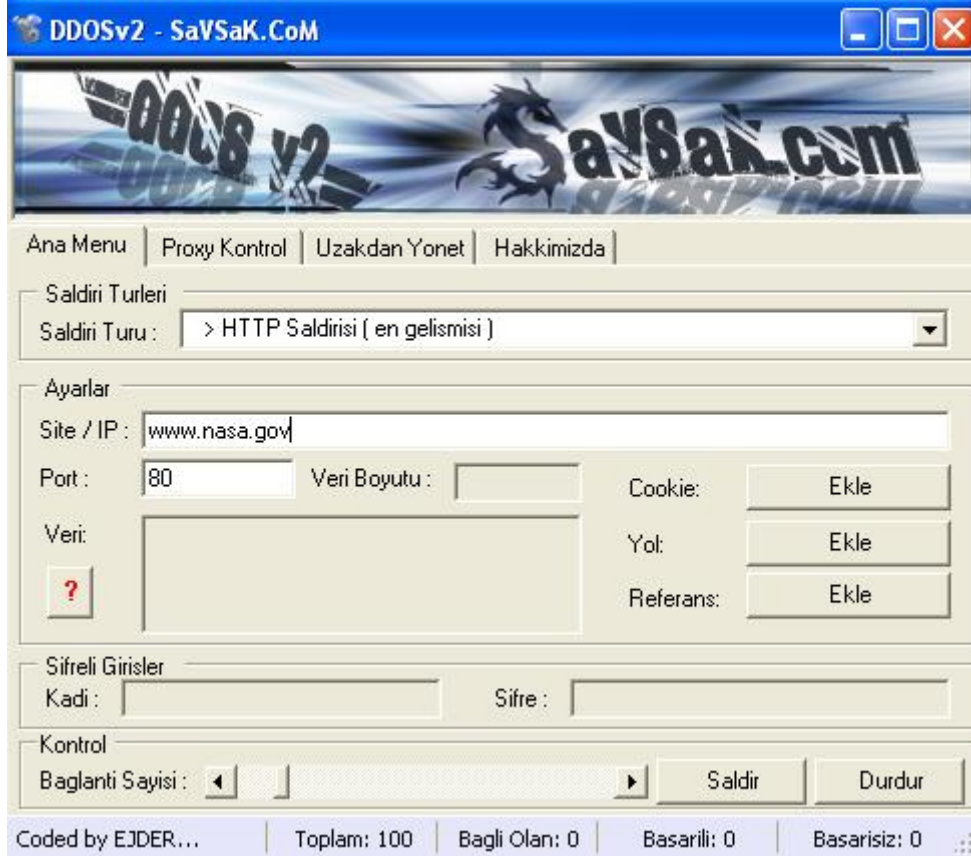


DDOS v2

Program Ejder tarafından, SaVSaK.CoM için yazılmıştır. Tüm hakları Ejder'e aittir. Programın kullanımı dolayısıyla gelecek zararların hiç biri Ejder ve Savsak.com'u ilgilendirmez.

8 çeşit saldırı modeline sahiptir. Bunlar kullanım yerleri ve özelliklerine göre birbirlerinden farklılık göstermektedir.



- HTTP Saldirisi (en gelismisi)

En gelişmiş saldırı modelimizdir. Her türlü site için geçerlidir. İsteğe bağlı cookie, referans, path ekleme özelliklerine sahiptir. En önemli özelliği 60+ a yakın farklı istekte bulunabilmesidir. İçerisinde 14 çeşit browser tanımı ve bir o kadar encoding, dil, path, referans sayıları ile çeşitlenmektedir. Burdaki amaç sabit bir saldırı değil, kendimizi bir network çıkışı olarak gösterip, saldırının etkisini arttırmaktır. Tek çeşit paket yerine, çok çeşitli farklı kişilerden, pçlerden geliyormuş izlenimi verip , saldırı boyutunu büyütülmektedir. Çok etkili bir saldırıya sahiptir. Özelliklerindeki Cookie değeri? Bize üyelikli sistemleri geçmemiz, o tür sitelerin iç kısımlarında saldırının mümkün olmasını sağlamaktadır. Cookie bildiğiniz gibi tanımlayıcı bilgidir. Saldırı yapacağını site nin , kritik sayfalarının yollarını path (yol) kısmına ekliyerekden, saldırının etkisi artırılabilir. Unutmayinki database işlemlerinin en çok işlenen , yapılan kısımlarına saldırılar , sitenin cokusunu hızlandıracaktır.

Site/IP : bu kisma , sitenin Domain adini yazmaniz gerek. Su sekilde -> www.siteadi.com gibi. Sakin site URLsi, full yazmayin. Saldiracagimiz sayfaları baska yerden ekliecez. 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 Snifferr, 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 saldiracagimiz sayfaları icermektedir. Domainden itibaren hangi dizinde ise o kisimlari yazmaniz gerekecek. Mesela saldiracagimiz 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 saldircaksanız, o zaman -> forum/memberlist.asp?get=all seklinde yazip eklemeniz gerek. Saldircaginiz sayfa sayisini ne kadar arttirirrsanız o kadar etkili olur. Ayrica saldiracaginiz sayfaların , Veritabani islemlerinin en cok yapildigi yerlere yapmanız , saldiri etkisini arttirmaktadır.

Referans: Bu kisim saldirinin hangi siteden geldigini bize gosterecektir. Kimi siteler bu ozelligi LOG lar, bizde saldirinin yerini ve turunu, capini, etkisini arttirmek 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 kısmi daha garip site yada saldiridigimiz yerin kendi site uzantilarini yazadigimiz taktirde, olusacak manzara? Saldirdigimiz yer , kendi kendine saldirmis gibi izlenim verecektir. DDOS oldugu anlasilmasi guc olacak ve cokus hizlanacaktır.

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.carcurhackteam.com/> seklinde ekliyelim. Eger birine camur atacaksak? O sitenin adini kesin yazin ☺ o oyle boyle saldiridigimiz yer tarafından farkedilcek. Birbirlerine dusurebiliriz ;)



- Veri Saldirisi

Site yada IP ye veri gondermemiz icindir. Eger siteye veri saldiri yapcaksanız, 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 icergini komple siz

belirliyorsunuz. Bununla post ve get saldırılarında gerçekleştirebilirsiniz. Çok kullanışlı bir özelliktir bu. Eğer bir bilgisayara veri gönderecekseniz, IP adresini, portunu ve gönderilecek veriyi yazmanız yeterlidir. Gönderilecek veri hex ise? Hex'e çevirip veri kısmına yazılacak göndermeniz gerekecektir. Bu kısım ile exploitleri çok güzel taklit edebilirsiniz.

- Normal

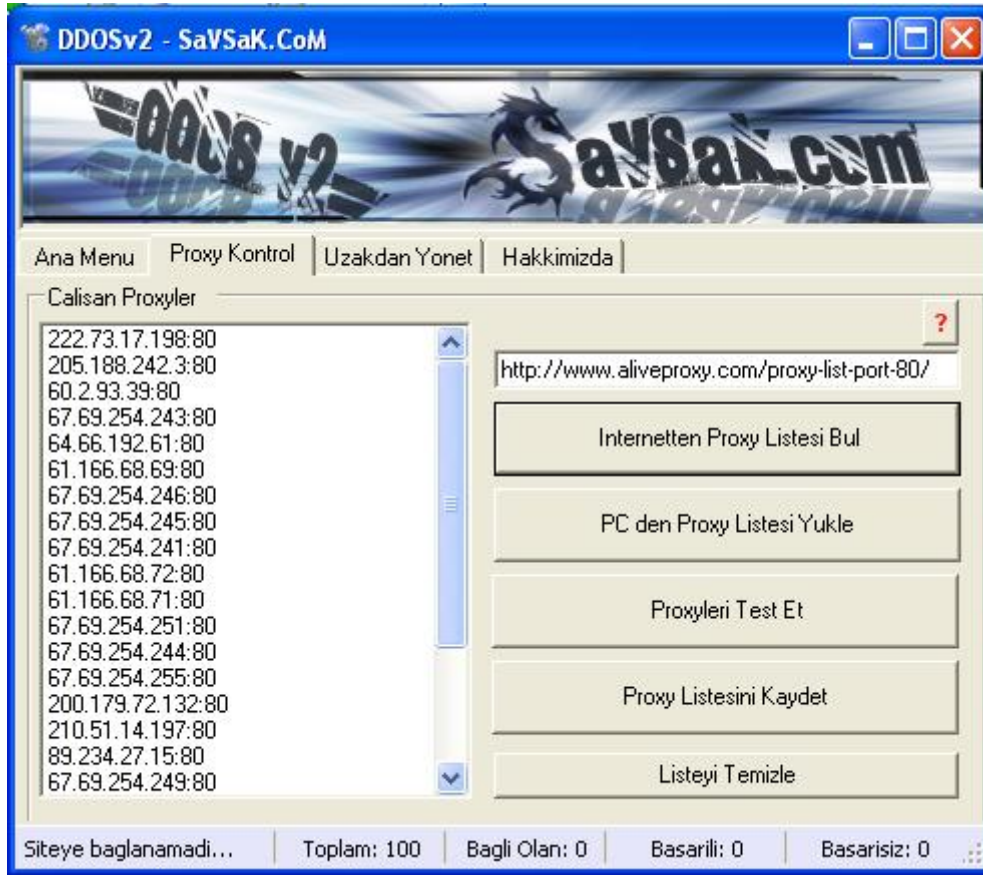
Bu ile diğerlerini birbirlerinden ayıran özellik? saldırı için kullanılan mimarıdır. HttpDdos saldırısında, socket yazılımı kullanılmaktadır. Sürekli socket yaratıp, karşılıksız kapamaktaydı. Şimdi bu seferki mimarıda, webrequest yapısını kullanılmaktadır. Bu diğerlerine oranla biraz yavaş kalabilir. Bunda sitenin kodları komple çekiliyor. Kıscası kaynak kod somuruyor. Bu saldırı seklide, çoklu saldırılar için etkili olacaktır. Bu saldırı mimarisine bazı özellikler ekliyerekden, protected Url saldırısı ve proxy saldırısı gerçekleştirilmektedir. Bu saldırıda sadece sitenin domain adını yazmanız yeterlidir. Direkt URL yazmanız yeterlidir. Mesela : <http://www.savsak.com/news.asp>

- Protected URL (Korumalı siteler için)

Bazı siteler, Protected URL yani şifre korumalı giriş özelliğini aktif etmektedir. O tür sitelere saldırmak için, geliştirdim bu yapıyı. Zaten sitelere giriş için gerekli şifre ve kullanıcı verilmektedir. Tek yapmamız gereken, saldıracağımız site Full url yazıp, kullanıcı ve şifre kısımlarını doldurup saldırıyı başlatmamızdır. Mesela : <http://www.savsak.com/news.asp>. Ne kadar çok kişi ile saldırırsak o kadar etkili ve hızlı çokme yasanız sitede.

- Proxyli

Proxyli Saldırı modelimizde, IP'mizi bir nevi korumak istenmiştir. Bu kısım için sadece saldıracağımız site URL'si yazmamız yeterlidir. Mesela : <http://www.savsak.com/news.asp>. Birde proxy listemizi eklememiz gerekir. Onuda ProxyKontrol kısmından ekliyoruz. O kısım için ya internetten çekerek, yada kendi localinizdekini yüklersiniz. İsterseniz check ettirirsiniz o size kalmış. Saldırı için Çalışan Proxyler kısmında proxy adresinin olmasıdır.



- RPCNUKE v2 Saldirisi - Win2000/XP

RPCNUKE exploitinin donusturulmus halidir. IP adresine saldiri mumkundur. Cok agir calismaktadır. 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 calismaktadır. Eger gerekli sartlar saglandi ise, saldiri baslamasi ile, makinanin yavaslamasi ve halt olmasi ile sonuclanmaktadır.

- MSSQL 7.0 DDOS sp0 - sp1 - sp2 - sp3

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

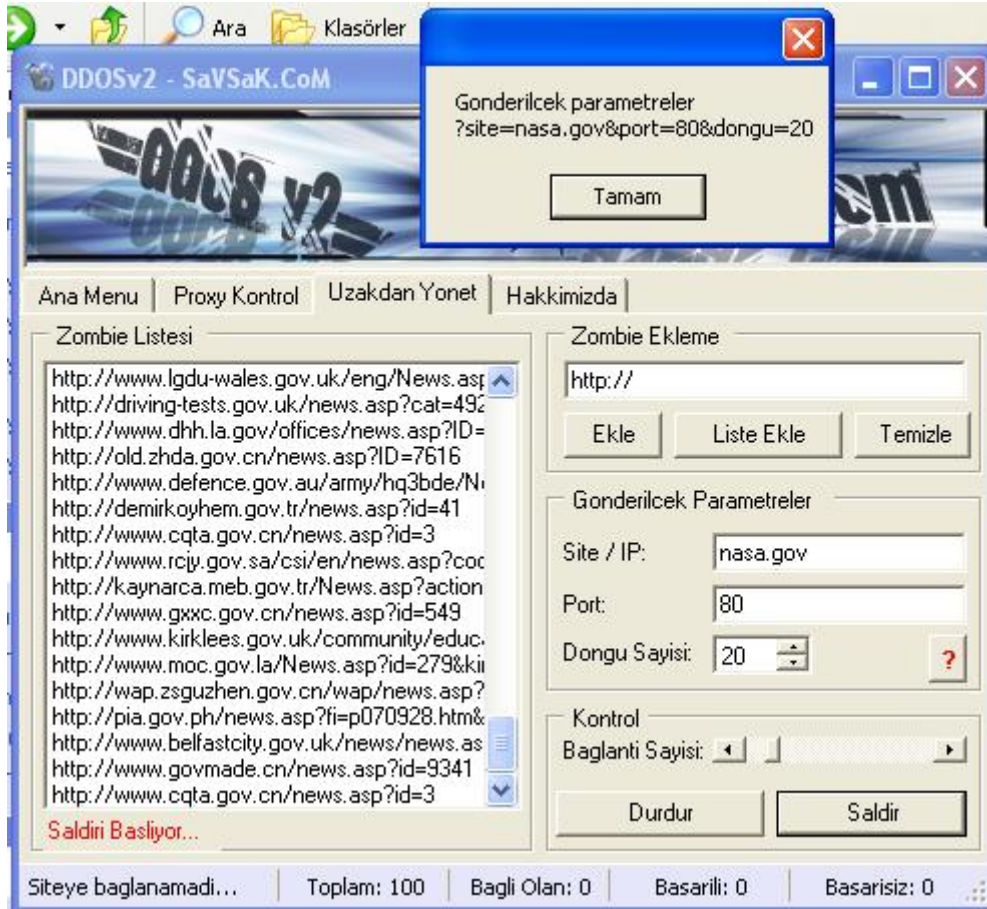
- Proxy Kontrol

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

- Uzakdan Yonet

Bu kisim ben Server lara yukledigimiz ufak shellciklerin kontrol edilip, toplu saldiri yapilmasi icin gelistirilmistir. Mesela Php, aspx de yazildigimi shelleri , hacklediginiz server

lara yukledikten sonra, onlari uzakdan bu programla listeye ekliyerekden, DDOS yapmanız mümkündür. Gonderdiği parametreler sabittir. O yuzden , gelen parametrelere gore, sizde kendi Shellini, ddos yaziliminizi yazabilirsiniz ve bu programla yönetebilirsiniz..



Kullanimia gelirse, server lara yuklediginiz shell adreslerini eklemeniz gerek listeye. Mesela; <http://www.savsak.com/ejder.php> gibi , eklemeniz gerek. Sonra Site/IP kismina , saldircaginiz DOMAIN i yazmanız gerek, www.saldirilcaksite.com gibi. Port kismina -> 80 olmalı. Dongu sayisi, shell kendi icinde kac kez donmesi gerektigidir. Saldirdiginizda, listedeki shellere, sıra ile veri gonderip, saldırmalarını gerçekleştirmektedir.



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

Program Ejder tarafından SaVSaK.CoM icin yazilmistir.

WwW.SaVSaK.CoM

by EJDER ;)

13 Kasim 2007