BGA

BİLGİ GÜVENLİĞİ AKADEMİSİ

Sızma Testlerinde İleri Düzey Teknikler

Ozan UÇAR

ozan.ucar@bga.com.tr

Ankara 2012

Konuşmacı Hakkında

- Bilgi Güvenliği Danışmanı ve Eğitmen
  - Bilgi Güvenliği AKADEMİSİ (www.bga.com.tr)
- Penetration Tester
- Blog Yazarı
  - blog.bga.com.tr
  - www.cehturkiye.com
- İletişim
  - Skype: ozan.ucar
  - Eposta: ozan.ucar@bga.com.tr
  - Twitter: #ucarozan

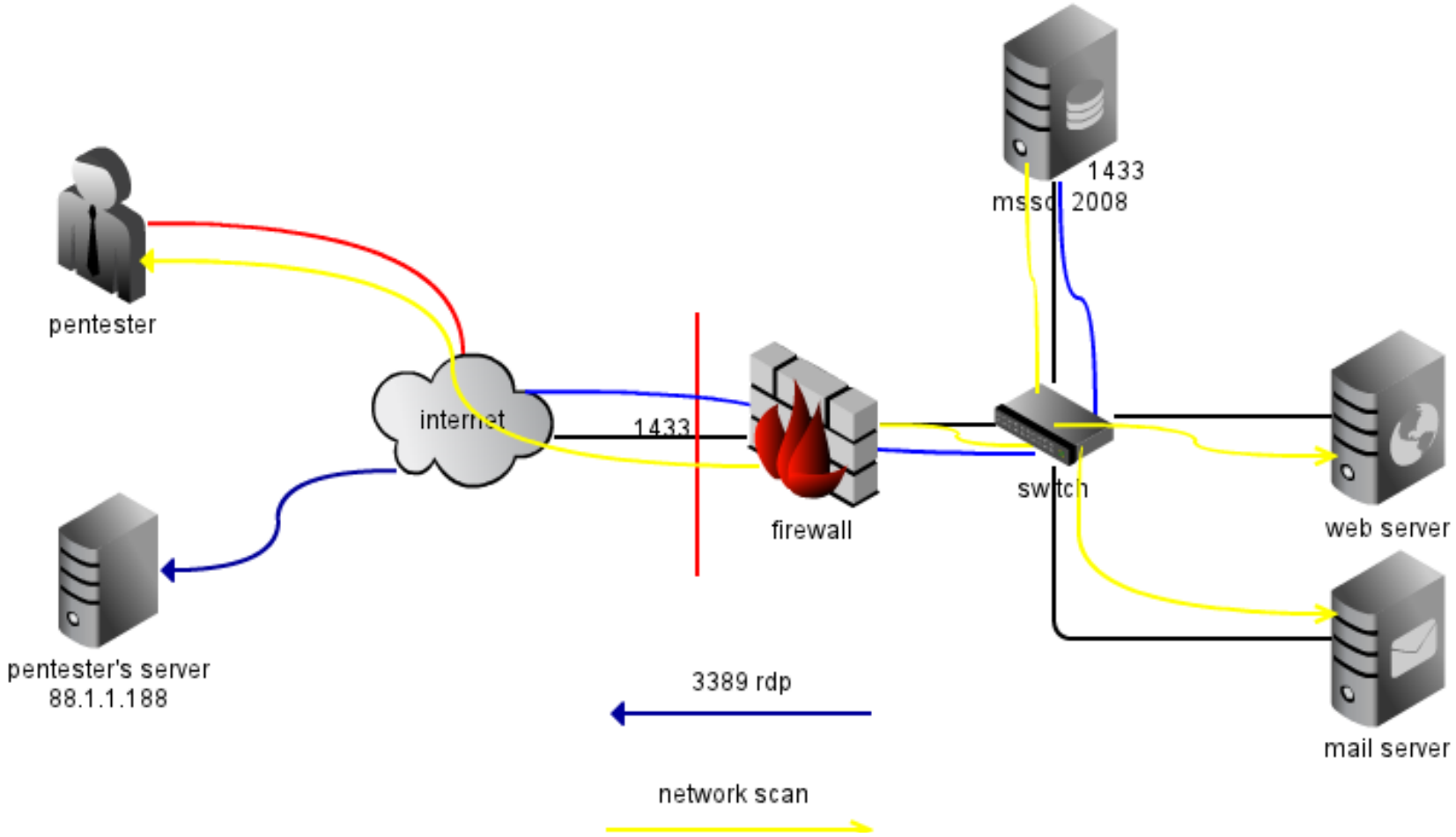
Notlar

- Sunum Süresi 45 dakikadır.
- Pratik Uygulamalar İçermektedir.
- Teknik ayrıntılar fazlaca yer almamaktadır.
- Sunum sonunda soru cevap kısmı olacaktır.

Senaryo

- BlackBox Pentest;
  - Basit parola kullanımı sonucu FTP sunucuya giriş yapılmıştır.
  - FTP'de bulan rapor.exe dosyası incelenerek hedefe ait sql bilgileri ele geçirilmiştir.
  - MSSQL sunucuya uzakdan bağlantı kurularak xm_cmdshell özelliği ile casus yazılım yüklenmiştir.
  - Casus yazılım aracılığı ile pivoting yapılarak hedef network dış dünyaya açılmış ve domain admin hakları ele geçirilmiştir.
  - Bu aşamadan sonra hedef networkde bulunan tüm bilgisayarlar kontrol altına alınmıştır.

Senaryo


1433
mssql 2008
pentester
internet
1433
firewall
switch
web server
mail server
pentester's server
88.1.1.188
3389 rdp
network scan

MSSQL xp_cmdshell

- xp_cmdshell, işletim sisteminde komut çalıştırmayı sağlayan bir özelliktir.
- Windows sistemlerde veritabanları genellikle Administrator veya SYSTEM yetkileri ile çalıştırılmaktadır.

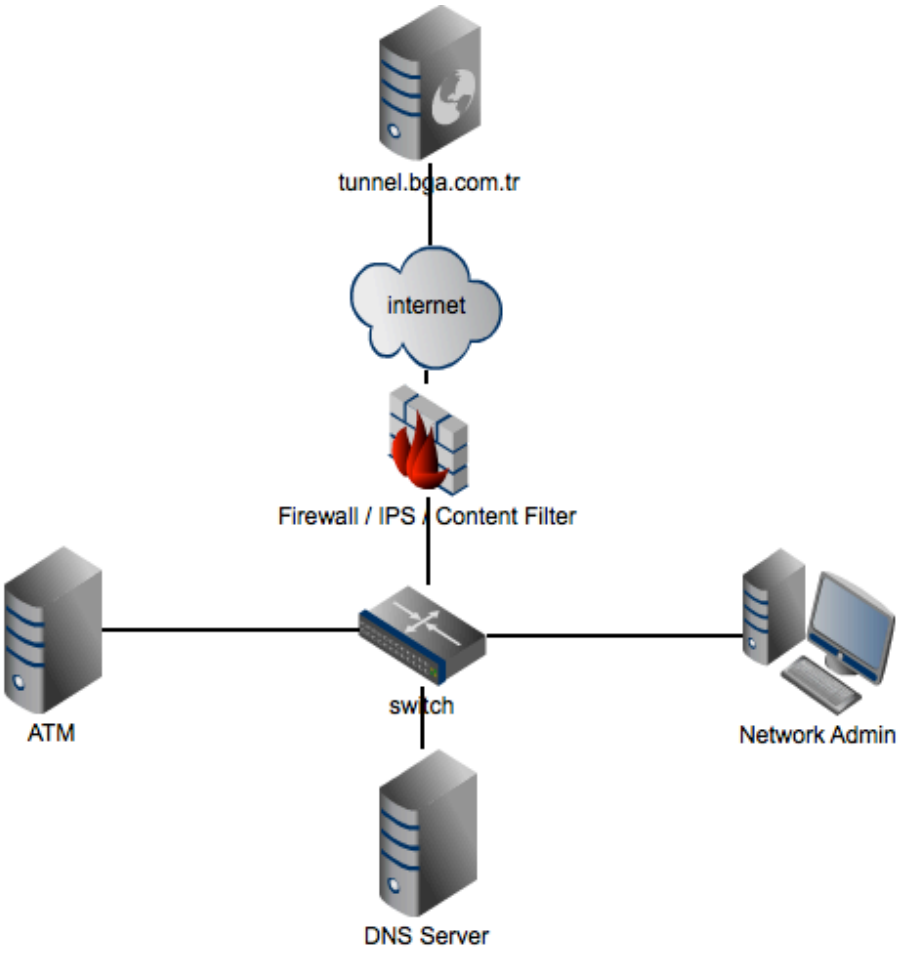
DNS Tunnel

- Veriler gerçek dns paketleri üzerinden taşınır.
- Paketler gerçek DNS paketleridir.
- DNS Payloadı içerisinde saldırganın dışarıya kaçırmak istediği veriler encrypt olarak saklanmaktadır.
- Dış dünyaya DNS sunucu üzerinden veri kaçırmak için başarılı bir yöntemdir.

DNS Tunnel

- Banka networkünde network admin bilgisayarına sosyal mühendislik yapılarak casus yazılım yerleştirilmiştir.
- Casus yazılım aracılığı ile network admin bilgisayarı üzerinden ATM bölgesindeki bir sistem ele geçirilmiştir.
- ATM'nin dış dünyaya erişimi tüm katmanlarda engellenmiştir.
- ATM sistemi, DMZ bölgesindeki DNS sunucuya paket gönderebilmekte ve yanıt alabilmektedir bu sayede DNS Tunnel ile dış dünyaya veri kaçırılmıştır.

DNS Tunnel


tunnel.bga.com.tr
internet
Firewall / IPS / Content Filter
ATM
switch
Network Admin
DNS Server

Network Pivoting

- Hedef networkü ters tünelleme yöntemi ile dış dünyaya açma işlemidir.
- IPS, Firewall, Content Filter, Antivirus, Kimlik Doğrulamalı Ağ Geçidi vb. tüm korumaları atlatacak tek bir TCP oturumu yeterlidir.

Captive Portal / DNS Tunnel

- Captive Portal diğer bir isimle HOTSPOT sistemleri kimlik doğrulamalı ağ geçididir.
- Kimlik doğrulamayı tamamlamayan kullanıcının, internet dünyasına tüm port/ protokolleri kapalıdır.
- Captive portal bir dns forwarder olduğu için DNS tunnel ile atlatılabilir.

Captive Portal / DNS Tunnel

File Edit View History Bookmarks Tools Help

https://10.100....0JicUsd9ILLRun0

https://10.100.10.10/cgi-bin/login?redirect=http%3a%2f%2fwww.exploit-db.com%2f&timeout=58200&gateway=10.100.10.10%3a5280

BackTrack Linux | Exploit-DB | Aircrack-ng | Offensive Security | SomaFM

TÜBİTAK kablosuz erişim için e-posta kullanıcı adı ve şifresini kullanınız. Misafir kullanıcılar ilgili linkten erişim sağlayabilirler.

Kullanıcı Adı:

Şifre:

GİRİŞ

MİSAFİR KULLANICI

TÜBİTAK

root@bt: /pentest/backdoors/iodine

File Edit View Terminal Help

```
Opened dns0
Opened UDP socket
Sending DNS queries for vpn.cehturkiye.com to 193.140.80.8
Autodetecting DNS query type (use -T to override).
Using DNS type NULL queries
Version ok, both using protocol v 0x00000502. Yo
Setting IP of dns0 to 5.5.5.2
Setting MTU of dns0 to 1130
Server tunnel IP is 5.5.5.5
Testing raw UDP data to the server (skip with -r
Server is at 37.1.145.34, trying raw login: ....
Using EDNS0 extension
Switching upstream to codec Base128
Server switched upstream to codec Base128
No alternative downstream codec available, using
Switching to lazy mode for low-latency
Server switched to lazy mode
Autoprobing max downstream fragment size... (ski
768 ok.. 1152 ok.. ...1344 not ok.. ...1248 not
t ok.. ...1164 not ok.. will use 1152-2=1150
Setting downstream fragment size to max 1150...
Connection setup complete, transmitting data.
Detaching from terminal...
root@bt:/pentest/backdoors/iodine#
```

root@bt: ~

File Edit View Terminal Help

```
root@bt:~# ping 5.5.5.1
PING 5.5.5.1 (5.5.5.1) 56(84) bytes of data.
^C
--- 5.5.5.1 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@bt:~# ping 5.5.5.5
PING 5.5.5.5 (5.5.5.5) 56(84) bytes of data.
64 bytes from 5.5.5.5: icmp_seq=1 ttl=64 time=96.3 ms
64 bytes from 5.5.5.5: icmp_seq=2 ttl=64 time=67.8 ms
64 bytes from 5.5.5.5: icmp_seq=3 ttl=64 time=62.0 ms
^C
--- 5.5.5.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 62.085/75.406/96.303/14.964 ms
root@bt:~#
```

Son Kullanıcıya Yönelik Saldırılar (1)

Azat Camlibel via LinkedIn member@linkedn.com 1 Kasım (5 gün önce)

Kime: bana

Azat Camlibel wants to consnect with you on LinkedIn.

74 shared connections

Azat Camlibel

Business Manager at Sales Force Europe View Profile »

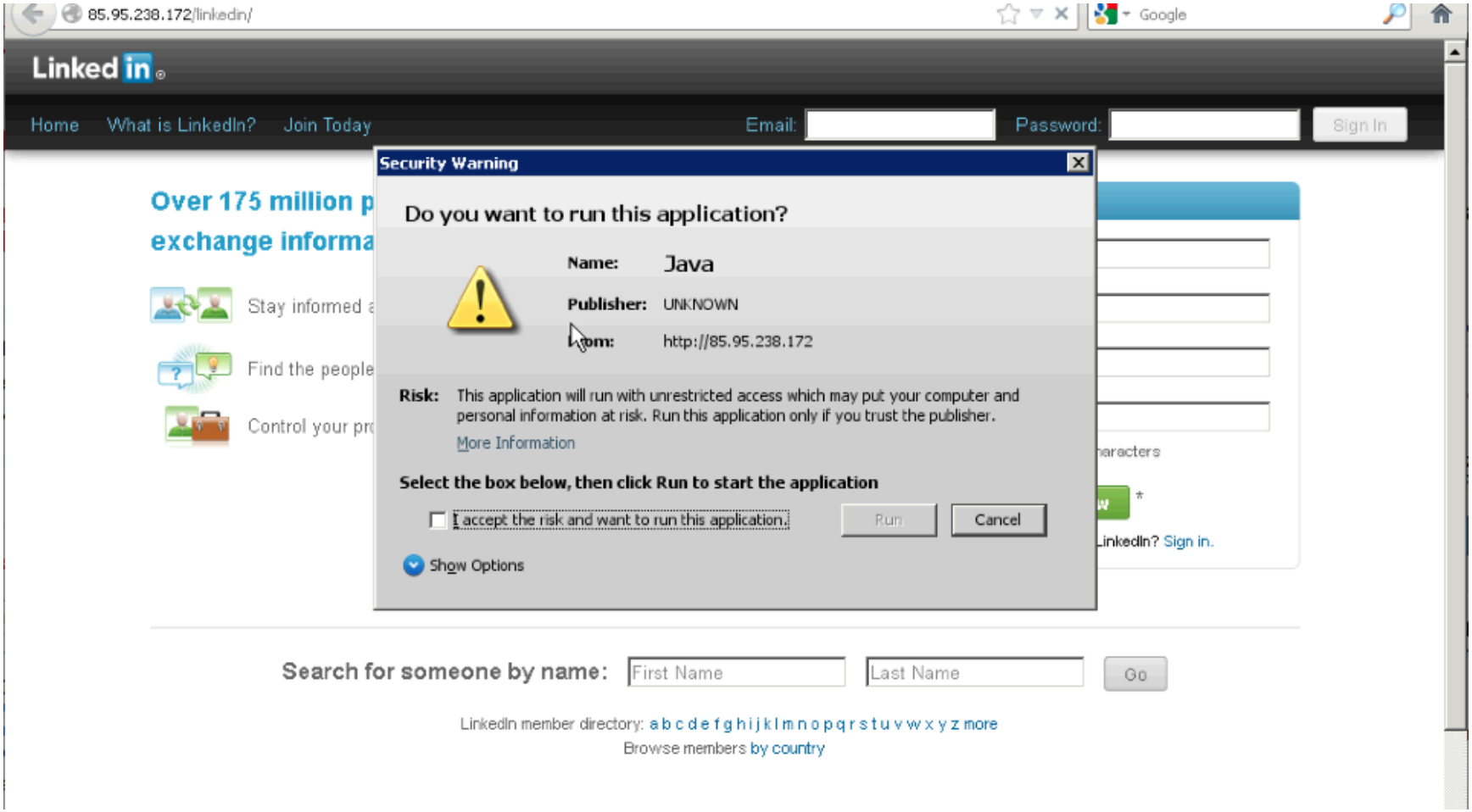
Accept

http://85.95.238.172/linkedin

Web Java Applet Attack

- Java multiplatform çalışan bir uygulamadır.
- Java applet ile hedef sistemde kod/komut çalıştırmak mümkündür.
- Son kullanıcının dikkatsizliğinden faydalanarak bir casus yazılım Java applet ile hedefe yüklenebilir.
- Kurbanın, Java uyarısına ‘RUN’ demesi yeterlidir.

Web Java Applet Attack



Son Kullanıcıya Yönelik Saldırılar (2)

Sayın ilgili,

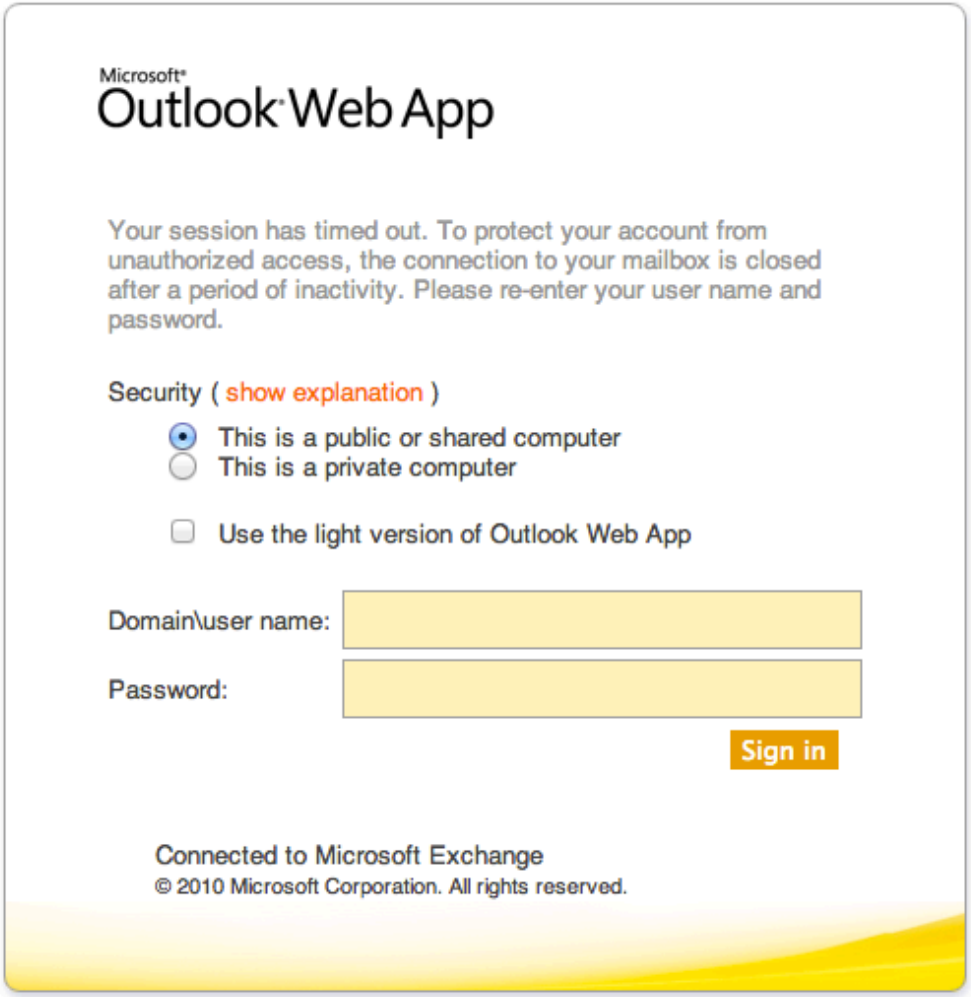
Şirket bünyesinde uzun süredir altyapı çalışmalarını yürütmekte olduğumuz yeni nesil e-posta ve iletişim sistemlerine bu hafta itibariyle geçiş yapmış bulunmaktayız. Kullanılan e-posta hesaplarında problem yaşanmaması adına aşağıda bağlantısı verilen OWA(Outlook Web Access) uygulamasına giriş yaparak hesabımı güncelle seçeneğini işaretlemeniz beklenmektedir.

OWA 2012 Giriş

Xyz Firması

Insan Kaynakları Yönetimi

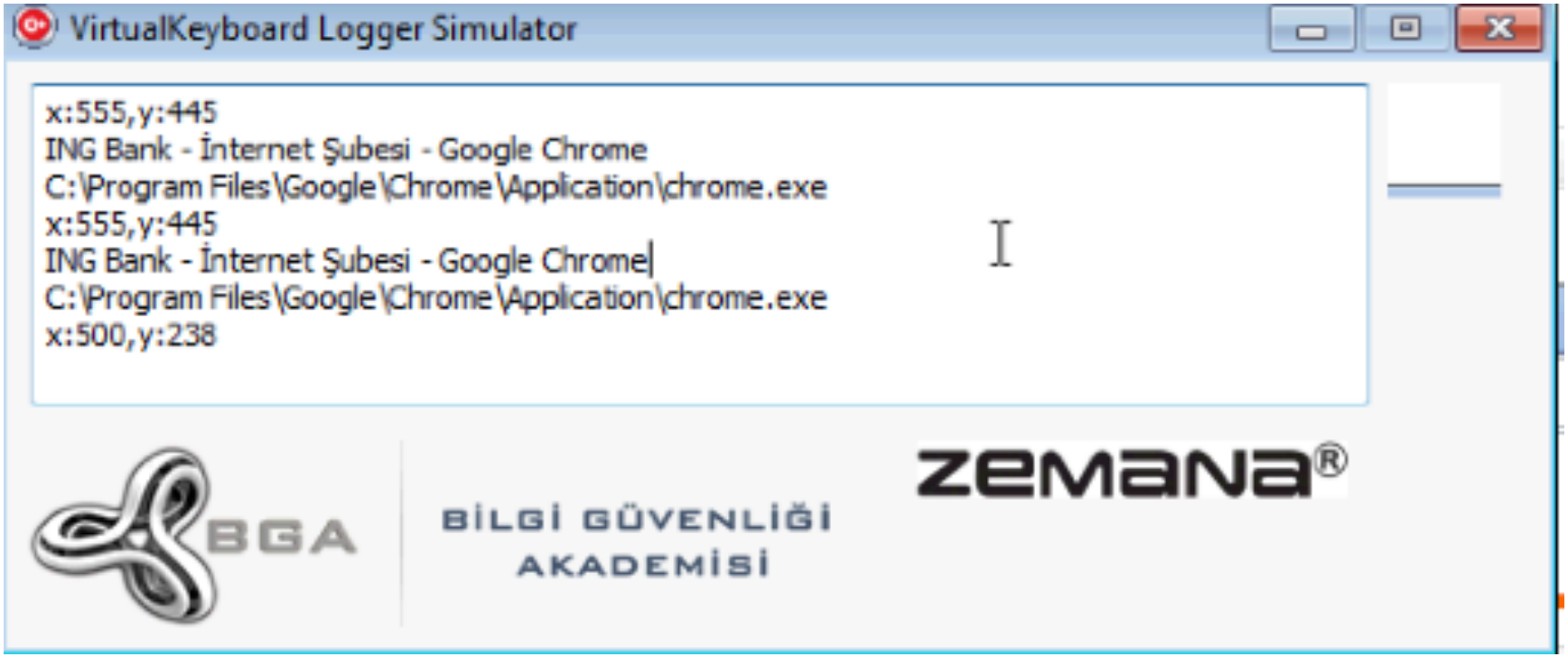
OWA Girişi


Microsoft
Outlook Web App
Your session has timed out. To protect your account from unauthorized access, the connection to your mailbox is closed after a period of inactivity. Please re-enter your user name and password.
Security (show explanation)
This is a public or shared computer
This is a private computer
Use the light version of Outlook Web App
Domain\user name:
Password:
Sign in
Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

Ajan Marmara

- Eğitim için geliştirilmiştir.
- Mouse haraketlerini takip eder.
- Sanal klavye casusluğu yapmaktadır.
- Antivirus ve Sezgisel Antilogger'lara karşı tanınma oranı 0/43
- Verileri saldırgana ait sunucuya POST eder.

Ajan Marmara



Ajan Marmara

85.95.238.173/keylog/upload.php

BGA BİLGİ GÜVENLİĞİ AKADEMİSİ zemana®

1	85.95.238.172	BGA-BILGISAYARBGA		Windows7x32	chrome.exe	ING BANK
2	85.95.238.172	BGA-BILGISAYARBGA		Windows7x32	chrome.exe	ING BANK
3	85.95.238.172	BGA-BILGISAYARBGA		Windows7x32	chrome.exe	ING BANK
4	85.95.238.172	BGA-BILGISAYARBGA		Windows7x32	chrome.exe	ING BANK
5	85.95.238.172	BGA-BILGISAYARBGA		Windows7x32	chrome.exe	ING BANK
6	85.95.238.172	BGA-BILGISAYARBGA		Windows7x32	chrome.exe	ING BANK
7	85.95.238.172	BGA-BILGISAYARBGA		Windows7x32	chrome.exe	ING BANK
8	85.95.238.172	BGA-BILGISAYARBGA		Windows7x32	chrome.exe	ING BANK
9	85.95.238.172	BGA-BILGISAYARBGA		Windows7x32	chrome.exe	ING BANK
10	85.95.238.172	BGA-BILGISAYARBGA		Windows7x32	chrome.exe	ING BANK

Teşekkürler

İstanbul 2012