İSTANBUL GELİŞİM ÜNİVERSİTESİ

Ekolojik, Ekonomik ve Sosyal Sürdürülebilirlik İçin

İstanbul Gelişim Üniversitesi

Siber Güvenlikte Su Saldırıları, Uygulamalı Ağ Sızma Testi ve Sosyal Mühendislik Saldırısı Eğitimi Etkinliği

Etkinlik Adı

Siber Güvenlikte Su Saldırıları, Uygulamalı Ağ Sızma Testi ve Sosyal Mühendislik Saldırısı Eğitimi Etkinliği

Sunum Konusu

Su Saldırıları (Watering Hole Attacks)

Dr.Öğr.Üyesi Hakan Aydın
İstanbul Gelişim Üniversitesi
Bilgisayar Mühendisliği
Bölüm Başkanı

Su Saldırıları (Watering Hole Attacks)

Siber Saldırıya Uğrayan

WEB Sayfaları

Siber Saldırgan

Su Saldırıları (Watering Hole Attacks)

- Bir web sitesinin hacklenmesi ve buraya gelen ziyaretçilerin tarayıcı, işletim sistemi, flash, java client'larının zafiyetlerinden faydalanarak ziyaretçilerin istemcilerine sızılması olarak açıklanabilir.

Su Saldırıları (Watering Hole Attacks)

- Bu siber saldırı tipinde, saldırganlar avlarını kovalamak yerine bir tuzak kurarlar ve avın kendilerine gelmesini beklerler.
- Saldırganların tuzak kurdukları yerler genellikle kurbanlarının sıklıkla ve düzenli olarak ziyaret ettikleri web site/sayfalarıdır.

Su Saldırıları (Watering Hole Attacks)

- «Watering Hole» ifadesi doğal dünyadaki avlarına sulama deliklerinin yakınında saldırmak için bir fırsat bekleyen avcılardan gelmektedir.
- Bu pasif-saldırı metodunu, musluğun başında bekleyen kötü niyetli birinin, sudan faydalanmak isteyip çeşme başına gelenleri avladığı bir saldırı modeli olarak tanımlayabiliriz.

Su Saldırıları (Watering Hole Attacks)

- Saldırganların hedefleri genellikle büyük işletmelerin, devlet dairelerinin vb. çalışanlarıdır.
- Saldırgan web sitelerindeki güvenlik açıklarını arar ve hedefi kötü amaçlı yazılımın barındırıldığı ayrı bir siteye yönlendiren kötü amaçlı JavaScript veya HTML kodu enjekte eder.

SU SALDIRILARI (Watering hole ATTACKS)

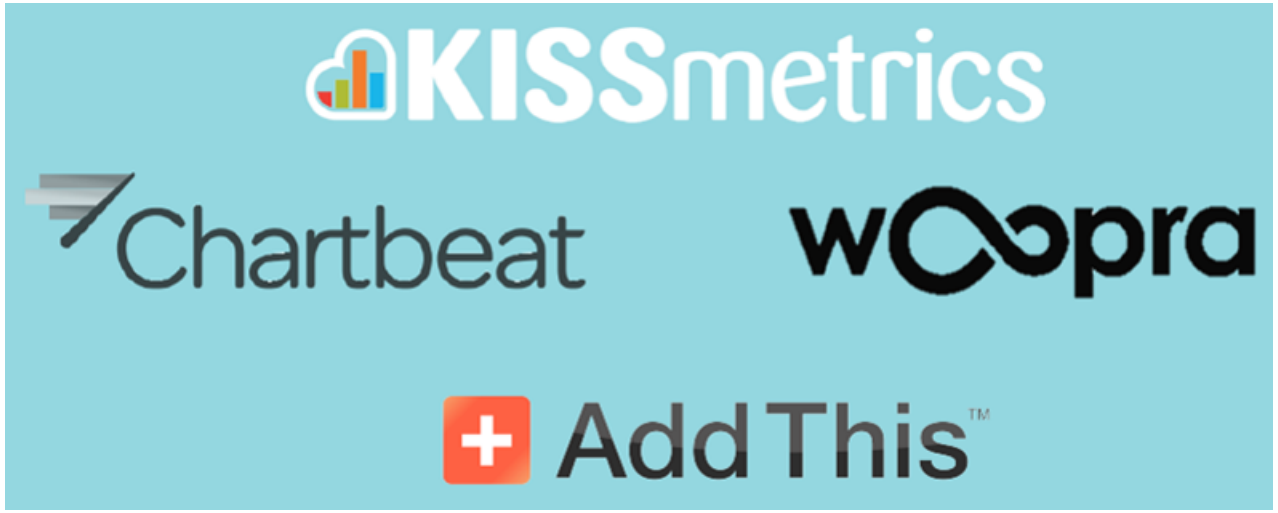
- Bu siber saldırı 4 (dört) ana aşamadan oluşmaktadır:
  - **1-** Araştırma / uygun ortam bulma
  - **2-** Yerleşme
  - **3-** İstemciye enjekte olma
  - **4-** Aksiyon

Su Saldırıları (Watering Hole Attacks)

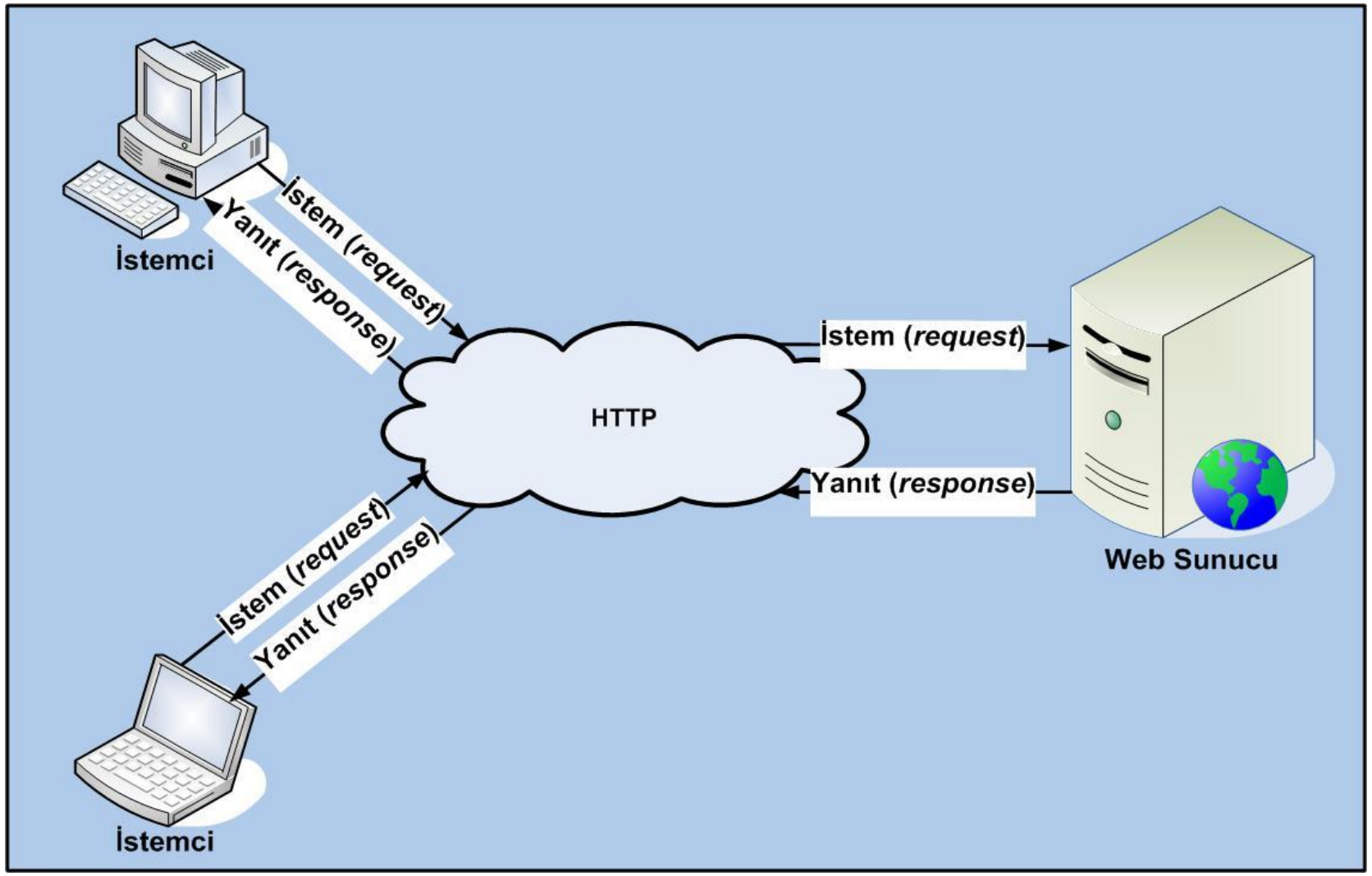
- **1.** Saldırganlar kurbanlarının düzenli ve sıklıkla ziyaret ettikleri web sitelerini saptar. (1nci Adım: Araştırma / uygun ortam bulma)
- **2.** Saptanan web sitesinin güvenlik zafiyeti aranır ve bulunduğunda «kötücül yazılımı" bu web site/sayfasına yerleştirilir. (2nci Adım: Yerleşme)
- **3.** Kurbanının ziyaret etmesini bekler. (3ncü Adım: İstemciye enjekte olma)
- **4.** Ya ziyaret sırasında zarara verilir ya da kötücül web sitesine yönlendirilir. (Son Adım: Aksiyon)

Su Saldırıları (Watering Hole Attacks)

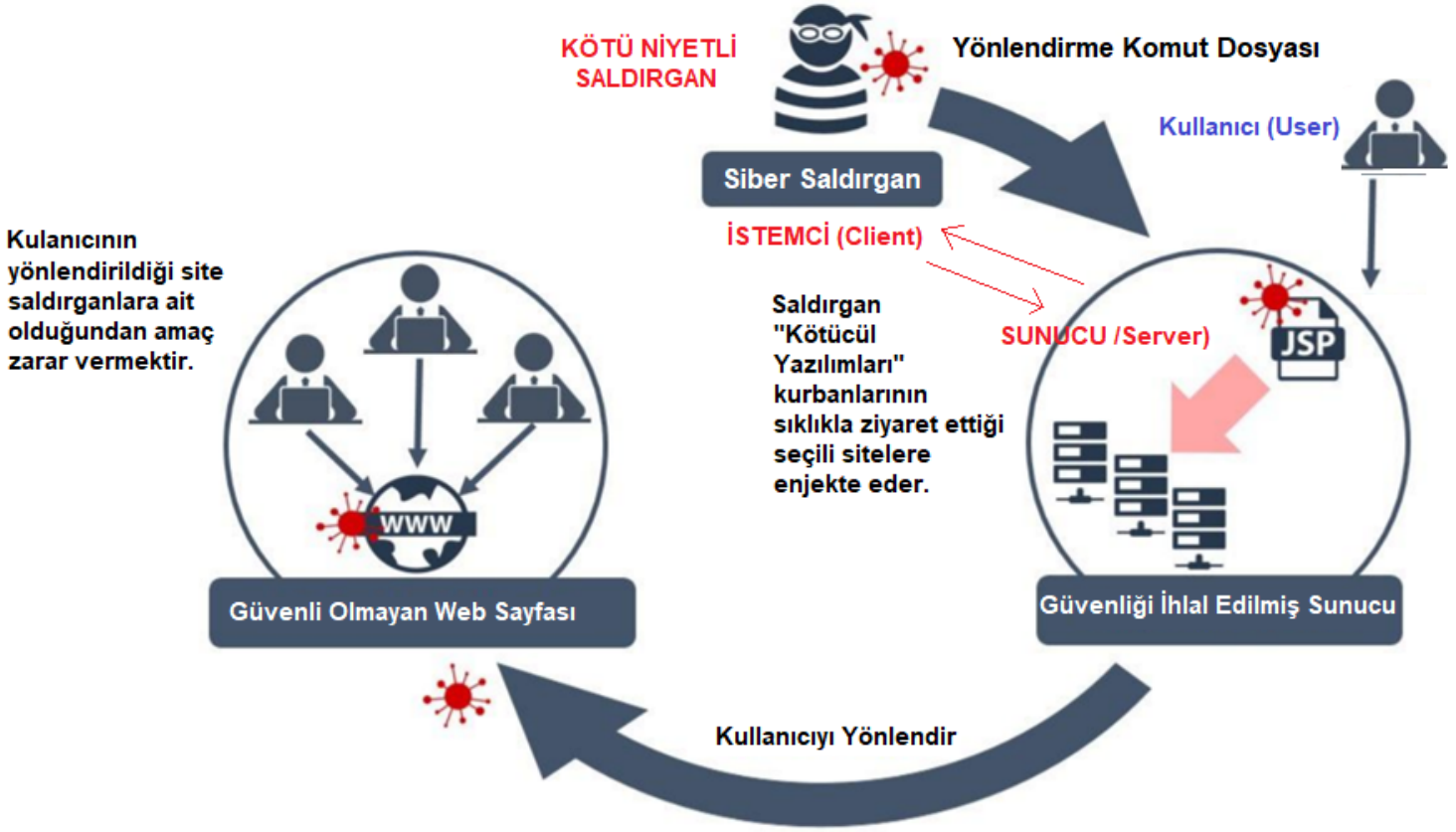
- Saldırganlar, hedef şirketlerinin çalışanları tarafından sık sık ziyaret edilen siteleri belirlemek için internet izleme yazılımlarını kullanırlar.



İSTEMCİ (Client) / SUNUCU (Server) MİMARİ



SU SALDIRILARI (Watering Hole ATTACKS)



Exploit Loader

The malicious html file checks for the presence of IE 10 with adobe flash. If the browser is IE 10 with flash installed then it loads a malicious flash file *(Tope.swf)*

checks for IE 10 with flash

Kötü amaçlı html dosyası, adobe flash ile IE10'un varlığını denetler. Tarayıcı, flash yüklü IE 10 ise, kötü amaçlı bir flash dosyası yükler (Tope.swf)

Malicious Flash Object

Flash triggers the exploit and downloads an image file (.jpg)

Flash, istismarı tetikler ve bir görüntü dosyası (.jpg) indirir

Su Saldırıları (Watering Hole Attacks)

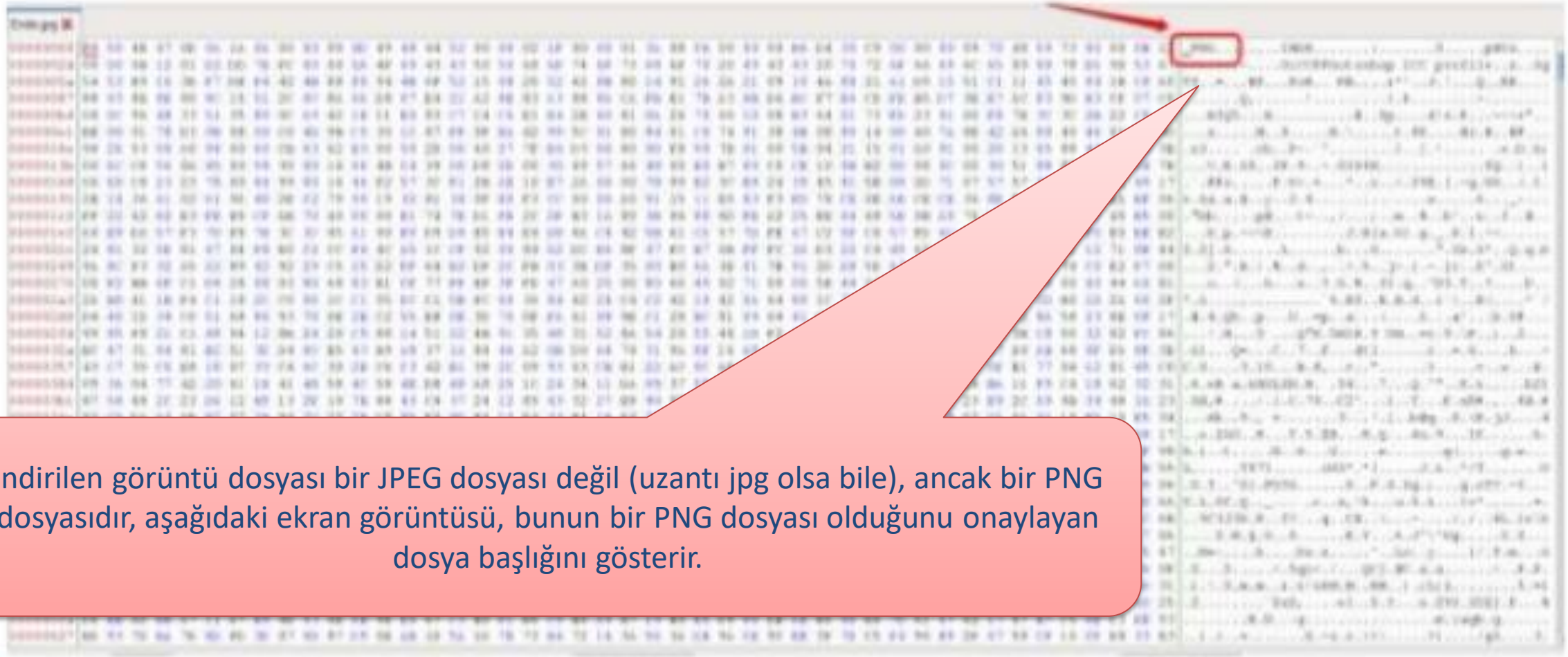
Örnek: Haberde, saldırganın ele geçirdiği sunucu üzerindeki «Whatsup», «Ccleaner», «Recuva» ve «TeamViewer» gibi yazılımları yüklemeye çalışan kullanıcıların uğradığı «Su Saldırısından» bahsedilmektedir.

Siber güvenlik uzmanları, yakın zamanda hacker grubu StrongPity'nin Türkiye ve Suriye'deki kurbanları hedef aldığını keşfetti. Hacker grubu, kullandığı "watering hole" saldırı tekniği ile WhatsApp, Ccleaner, Recuva ve TeamViewer gibi yazılımları yüklemeye çalışan kullanıcıların bilgisayarlarına kolayca giriş yapıyor ve bulaştığı bilgisayardaki dosyaları toplayıp dışarıya gönderiyor.

İlginç bir şekilde araştırılan tüm dosyalar, Pazartesi-Cuma arası 9-6 çalışma saatleri arasında derlenmiş gibi görünüyor. Bu da çeşitli projeler yürütmek için tam zamanlı çalışan sponsorlu bir yazılım firması olabileceği fikrini destekliyor.

Image file is a png file

The image file downloaded is not a JPEG file (even though the extension is .jpg) but a PNG file, the below screenshot shows the file header which confirms its be a PNG file



İndirilen görüntü dosyası bir JPEG dosyası değil (uzantı jpg olsa bile), ancak bir PNG dosyasıdır, aşağıdaki ekran görüntüsü, bunun bir PNG dosyası olduğunu onaylayan dosya başlığını gösterir.

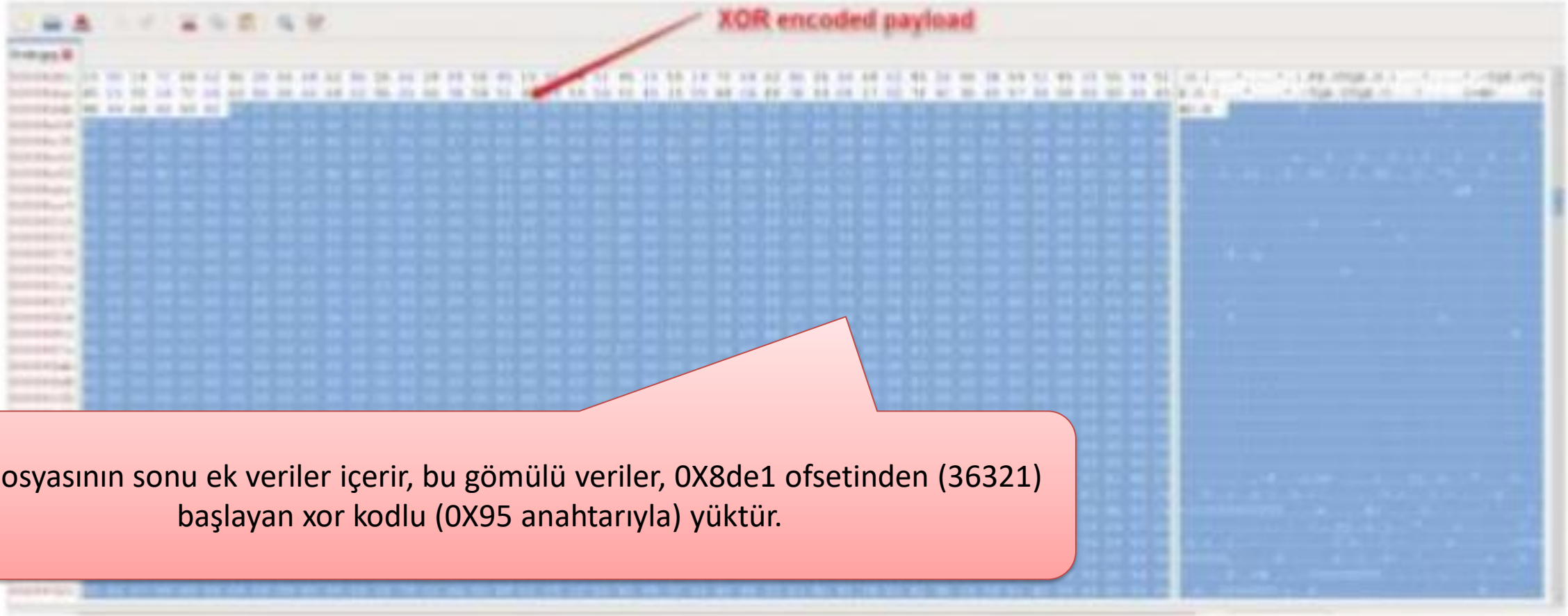
Image file used in the attack

The below screenshot shows the image file that was used in the attack.

Ekran görüntüsü, saldırıda kullanılan görüntü dosyasını göstermektedir.

Image file contains additional data

The end of the PNG file contains additional data, this embedded data is the xor encoded (with key 0x95) payload starting at offset 0x8de1 (36321)



PNG dosyasının sonu ek veriler içerir, bu gömülü veriler, 0X8de1 ofsetinden (36321) başlayan xor kodlu (0X95 anahtarıyla) yüktür.

Script to extract and decode content

Simple script to extract and decode the additional content starting at offset 0x8de1 (36321).

```
def xor_decode(content, key):
    decoded = ""
    for ch in content:
        if ch == "\x95" or ch == "\x00":
            decoded += ch
        else:
            decoded += chr(ord(ch) ^ key)
    return decoded


key = 0x95
fr = open(r'/root/Desktop/IE_zero/Eridо.jpg', 'rb')
fw = open(r'/root/Desktop/IE_zero/decoded.bin', 'wb')

content = fr.read()
encoded_content = content
```

0X8de1 (36321) ofsetinden başlayarak ek içeriği ayıklamak ve çözmek için basit komut dosyası.

Su Saldırıları (Watering Hole Attacks) – Siber Savunma

- WEB faaliyetlerinizi izleyen ve takip eden uygulama ve hizmetlerin tanımlanması ve bunların engellenmesi,
- Http yeniden yönlendirmelerini engelleyen tarayıcı eklentilerinin kullanımı,
- WEB Tarayıcıları için otomatik güncellemelerin etkinleştirilmesi,
- Tüm hizmetlerin görünür olmasının sağlanması.

İSTANBUL GELİŞİM ÜNİVERSİTESİ

Katılımınız İçin

Teşekkür Ederiz.

Ekolojik, Ekonomik ve Sosyal Sürdürülebilirlik İçin

İstanbul Gelişim Üniversitesi

www.gelisim.edu.tr gelisimedu igugelisim