ALTAY TAKIMI

PCAP ANALİZİ RAPORU

Hazırlayan : Efe Körün

Tarih : 16.03.2025

OLAY/VAKA ÖZETİ

Bu olay, **19 Temmuz 2019** tarihinde, **mind-hammer.net** şirket ağındaki **172.16.4.205** ip adresli **rotterdam-pc** adlı bilgisayardaki **matthijs.devries** adlı kullanıcı hesabı tarafından sahte bir tarayıcı güncellemesi adı altında kötü amaçlı bir phishing web sitesinden **SocGholish** adlı zararlı zararlı bir JavaScript dosyasının indirmesi ve çalıştırması ile gerçekleşmiştir. Bu dosya çalıştırıldığında NetSupport Manager adlı bir uzaktan erişim application'unun kötüye kullanılan bir versiyonunu sisteme yerleşmiştir. Bu sayede saldırganlar, hedef bilgisayara tam erişim sağlamış ve kontrolü ele geçirmiştir.

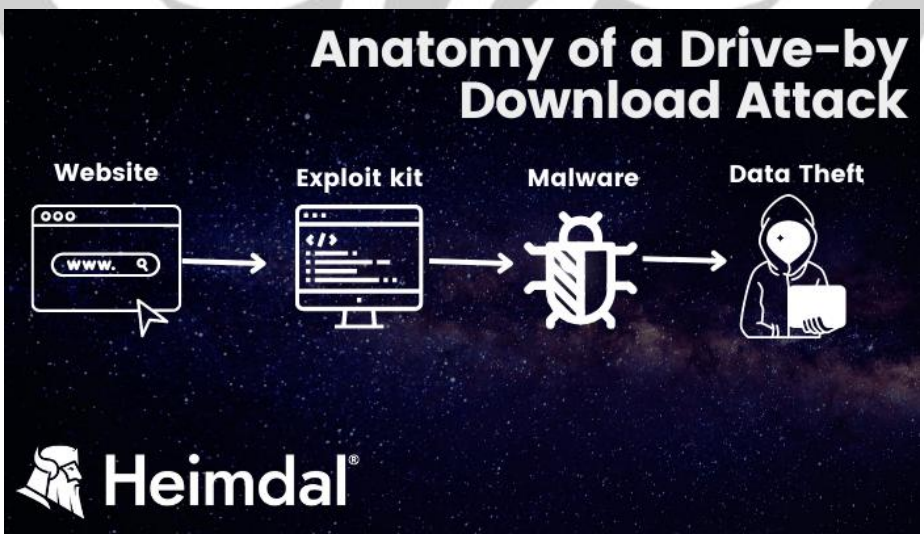
DETAYLI ANALİZ

Kurban Bilgisayar Bilgileri:

- ➤ **IP Adresi:** 172.16.4.205
- ➤ **MAC Adresi:** 00:59:07:b0:63:a4
- ➤ **Bilgisayar Adı:** ROTTERDAM-PC
- ➤ **Kullanıcı Hesabı:** matthijs.devries
- ➤ **Şirket Bilgisi:** Mind-Hammer
- ➤ **Şirket Domain Bilgisi:** mind-hammer.net
- ➤ **Windows Sürümü:** Windows 7

Saldırının Gerçekleşme Vektörü ve Akışı:

Zararlı yazılım bulaşma süreci incelendiğinde, tipik bir "drive-by download" ve sosyal mühendislik tekniklerinin kullanıldığı görülmektedir.



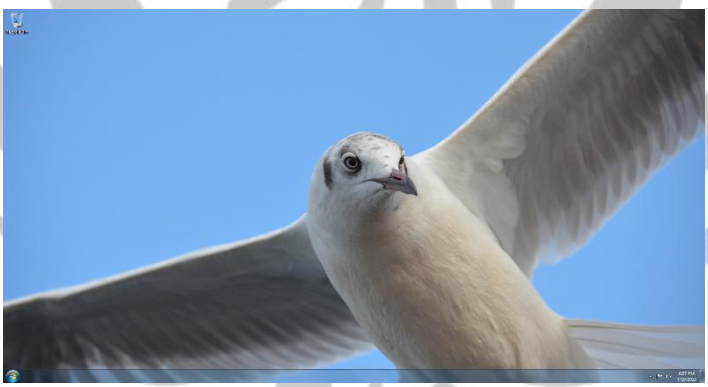
1. **matthijs.devries** adlı kullanıcı, 18:52 saati sıralarında "**mysocalledchaos.com**" adlı web sitesini ziyaret etti ve bu site, muhtemelen daha önceden zararlı yazılım bulaştırılmış, zaafiyeti sömürülmüş bir siteydi.

Siteyi ziyaret ettiğinde, 166.62.111.64 IP adresinden gelen bir JavaScript web enjeksiyonu gerçekleşti ve bu enjeksiyon, kullanıcının tarayıcısının güncellenmeye ihtiyacı olduğunu belirten sahte bir bildirim gösterdi.

Kullanıcı güncelleme bağlantısına tıkladığında, 81.4.122.101 IP adresinden **Let's Encrypt Free SSL** sertifikası kullanılarak güvenli görünmesi sağlanmış "ball.dardavies.com" domain adını kullanan 93.95.100.178 IP adresine yönlendirildi.

Kullanıcı, sahte güncelleme sayfasından bir zip dosyası indirdi ve bu dosyayı açtı. Zip içerisindeki zararlı JavaScript (.js) dosyasını çalıştırdığında, bilgisayar üzerinde zararlı kod çalışmaya başladı.

İlk üç POST isteği hexadecimal formatında veri gönderirken, sonraki iki istek ("empty.gif?ss&ss1img" ve "empty.gif?ss&ss2img") PNG formatında ekran görüntüleri iletti. Bu görüntülerden birinde, kullanıcının masaüstü arka planının ekran görüntüsü olarak pcap dosyasından çıkarılmıştır.



Zararlı kod çalıştıktan sonra, saat 18:53 sıralarında bilgisayar, 185.243.115.84 IP adresindeki bir sunucuya HTTP POST istekleri göndermeye başladı. Bu istekler "empty.gif" adlı bir dosyaya yönlendirilmişti.

Saldırganlar, topladıkları bilgiler doğrultusunda saat 18:57 UTC'de NetSupport Manager RAT (Remote Access Tool) zararlı yazılımını sisteme yüklemeyi başardılar.

NetSupport Manager kurulduktan sonra, 31.7.62.214 IP adresindeki sunucu ile 443 portu üzerinden iletişime geçti ve saldırganların uzaktan sisteme erişim sağlamasına olanak tanıdı.

Trafik analizinde, 6442 adet "NetSupport Remote Admin Checkin" uyarısı tespit edilmiştir. Bu durum, zararlı yazılımın uzun süre aktif kaldığını ve saldırganların sisteme defalarca erişim sağladığını göstermektedir.

TEHLİKE GÖSTERGELERİ (IOC'LER)

İlişkili IP Adresleri:

➤ 166.62.111.64: İlk zararlı JavaScript web inject dağıtımı için kullanılan IP adresi

➤ 81.4.122.101: SocGholish yönlendirme trafiğinde kullanılan IP adresi (kötü amaçlı SSL sertifikası ile)

➤ 93.95.100.178: Sahte güncelleme sayfasının barındırıldığı sunucu

➤ 185.243.115.84: Zararlı yazılımın ana komuta kontrol sunucusu, "empty.gif" dosyasına POST istekleri gönderilen hedef

➤ 31.7.62.213/214: NetSupport Manager RAT'ın iletişim kurduğu c2

İlişkili Domain ve URL'ler:

➤ ball.dardavies.com: Sahte güncelleme sayfasının barındırıldığı domain adı

➤ mysocalledchaos.com: Muhtemelen başlangıçtaki zararlı yazılım dağıtımının gerçekleştiği güvenlik açığı bulunan web sitesi

Tespit Edilen Zararlı Yazılım Aktiviteleri:

➤ SocGholish/FakeUpdates - Tarayıcı güncellemesi gibi görünen sahte güncelleme sayfaları aracılığıyla JavaScript tabanlı zararlı yazılım dağıtımı

➤ empty.gif dosyasına yapılan şüpheli POST istekleri - kurban bilgisayarın ekran görüntüleri dahil gif dosyası ile c2 sunucularına veri sızdılırması.

➤ NetSupport Manager RAT - Ticari bir uzaktan yönetim aracı olmasına rağmen, kötü amaçlı olarak bilgisayara yerleştirilmiş ve çalıştırılmıştır