Pcap Analizi

Hazırlayan: Saliha Polat

Tarih: 15.03.2025

Olay/Vaka Özeti

19 Temmuz 2019 tarihinde, bir Windows kullanıcısı (172.16.4.205 – ROTTERDAM-PC) saldırıya uğramış bir web sitesini (mysocalledchaos.com) ziyaret etti. Kullanıcı, bu sayfadaki yönlendirmeye inanarak sahte bir güncelleme dosyasını indirdi.

İndirilen dosya, ZIP formatında bir arşiv olup içinde bir JavaScript (.js) dosyası barındırıyordu. Kullanıcının bu dosyayı çalıştırmasıyla birlikte sistemine zararlı yazılım bulaştı. Olayın ardından ağ trafiğinde anormal hareketler gözlemlendi.

166.62.111.64 adresinden gelen zararlı JavaScript web enjeksiyonu tespit edildi. Ardından sistem, Let's Encrypt sertifikası kullanılarak şifreli bir bağlantı kurdu. Bu, saldırganların yasal görünümlü HTTPS bağlantıları kullanarak zararlı dosya veya komutları aktardığını gösterdi.

Zararlı yazılımın çalıştırılmasının ardından, enfekte sistem 185.243.115.84 adresine HTTP POST istekleri göndermeye başladı. Daha sonra, enfekte sistem 31.7.62.214 adresine bağlantı kurarak NetSupport Manager RAT zararlısını yükledi. IDS/IPS sistemleri tarafından tespit edilen "NetSupport Remote Admin Checkin" ve "NetSupport Remote Admin Response" uyarıları, sistemin artık saldırganların kontrolüne geçtiğini gösterdi.

Detaylı Analiz

Kurban Ayrıntıları

Hostname: ROTTERDAM-PC

IP Addresi: 172.16.4.205

MAC Adresi: 00:59:07:b0:63:a4

User Account: matthijs.devries

Şirket ve Domain Bilgileri

Şirket: Mind-Hammer

Domain: mind-hammer.net

Domain Controller: 172.16.4.4

Gateway: 172.16.4.1

Broadcast: 172.16.4.255

Zararlı Türü

Windows Sürümü: Windows7 ya da 10

Saldırı Yöntemi: SocGholish

Son Yüklenen Zararlı Yazılım: NetSupport Manager RAT

Tehlike Göstergeleri (IOC'ler)

NetSupport RAT'ın C2 Sunucusu: 31.7.62.214

Sahte Güncelleme Bulunduran Alan Adı: ball.dardavies

Güncelleme için yüklenen zararlı ZIP

İçinde zararlı bulunan gif dosyası : /empty.gif?ss&ss1img, /empty.gif?ss&ss2img

Certificate