Network Analiz

Hazırlayan: Sinan Kocagöz

Hazırlama Tarihi: 15.03.2025

İçindekiler Tablosu

1. OLAY/VAKA ÖZETİ

19 Temmuz 2019 tarihinde saat 18:52 UTC'de mind-hammer.net domain ağında bir bilgisayar (172.16.4.205), SocGholish kötü amaçlı yazılımı tarafından enfekte edilmiştir. Saldırı, kötü amaçlı bir JavaScript enjeksiyonu ile başlamış ve NetSupport Remote Admin aracının kurulmasıyla sonuçlanmıştır. Bu uzaktan erişim aracı (RAT), saldırganların sistemde kalıcılık kazanmasını ve kontrol sağlamasını mümkün kılmıştır.

2. DETAYLI ANALİZ

➢ Kurban Bilgisayar Detayları:

- IP Adresi: 172.16.4.205
- MAC Adresi: 00:59:07:b0:63:a4
- Ana Bilgisayar Adı (Hostname): LenovoEMCPro
- Windows Kullanıcı Hesabı: [Bulamadım]
- Windows Sürümü: Windows 7 (User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0))
- Ağ Segmenti: 172.16.4.0/24
- Domain: mind-hammer.net

➢ Saldırı Vektörü ve Akışı:

1. İlk Enfeksiyon: SocGholish JavaScript web enjeksiyonu (166.62.111.64 adresinden)
2. Kötü Amaçlı SSL Sertifikalarıyla Bağlantılar: Let's Encrypt SSL sertifikaları kullanan şüpheli domainler üzerinden (81.4.122.101 ve 93.95.100.178)
3. Veri Sızdırma: GIF dosyalarına POST istekleri yoluyla veri aktarımı (185.243.115.84 adresine)
4. Kötü Amaçlı Yazılım Yükleme: NetSupport Remote Admin aracının kurulumu
5. Komuta Kontrol İletişimi: 31.7.62.214 IP adresi ile yüksek sayıda iletişim (6442 olay kaydı)

➢ Zararlı Yazılım Türleri:

- Birincil Enfeksiyon: SocGholish (Sosyal mühendislik temelli JavaScript kötü amaçlı yazılımı)
- İkincil Yük: NetSupport RAT (Uzaktan Erişim Aracı)

3. TEHLİKE GÖSTERGELERİ (IOC'LER)

➢ Kötü Amaçlı IP Adresleri:

- 166.62.111.64 - İlk SocGholish JavaScript enjeksiyonu kaynağı
- 81.4.122.101 - Kötü amaçlı SSL sertifikası (SocGholish yönlendirmesi)
- 93.95.100.178 - Şüpheli aktivite için Let's Encrypt SSL sertifikası kullanan
- 185.243.115.84 - GIF'e POST yoluyla veri sızdırma hedefi
- 31.7.62.214 - NetSupport komuta kontrol sunucusu