ALTAY

PCAP ANALİZ

OLAY VAKA RAPORU

15.03.2025

MEHMET MERMER

SİBERVATAN

OLAY VAKA ÖZETİ

2019-07-19/18:52 tarihinde 172.16.4.205 IP adresli bilgisayar sosyal mühendislik saldırısıyla karşı karşıya kalmıştır. SocGholish ile yapılmış bu saldırı sahte yazılım güncellemeleri yoluyla kötü amaçlı yazılım bulaştıran bir **s**osyal mühendislik saldırısıdır. Bilgisayara Zararlı JavaScript kodları içeren bir web sitesinden kötü amaçlı yazılım indirilmiştir. NetSupport Remote Admin uzaktan erişim (RAT) aracı sisteme yerleşmiştir. Ayrıca, bir görüntü dosyası (GIF) aracılığıyla veri sızdırma işlemide gerçekleştirilmiştir.

DETAYLI ANALİZ

Kurban Bilgisayar Ayrıntıları;

IP Adresi: **172.16.4.205**
MAC Adresi: **00:59:07:b0:63:a4**
Hostname: **Rotterdam-pc**
Win Kullanıcı Hesabı: **matthijs.devries**
Win Sürümü: -
Şirket Domain: **mind-hammer.net**

Zararlı Atak Vektörü:
SocEng/Gholish JS Web Inject Inbound ; Sosyal mühendislik saldırısıyla zararlı JS yazılımı.
NetSupport Remote Admin Checkin ; Remote Access Trojan uzaktan erişim aracı.

TEHLİKE GÖSTERGELERİ (IOC'LER)

Zararlı IP Adresleri;

- 166.62.111.64 - **SocEng/Gholish JS Web Inject Inbound Zararlı JS dosyası inmiş.**
- 81.4.122.101 **- Sahte SSL Sertifikası kötü amaçlı bir HTTPS trafiği oluşturmuş.**
- 93.95.100.178 - **Let's Encrypt sertifikası ile şifrelenmiş zararlı bağlantı**.
- 185.243.115.84 - **Verilerin bir GIF dosyasına POST edilmesi.**
- 31.7.62.214 **- NetSupport Manager gibi bir uzaktan yönetim aracı.**