PCAP DOSYA ANALİZİ

HAZIRLAYAN:MUHAMMED ALİ ZENGİN
17.03.2025

OLAY ÖZETİ

172.16.4.205 cihazı SocGholish zararlısı indiridi. Ardından Let'sEncrypt SSL sertifikaları kullanılarak kötü amaçlı trafik gerçekleşti ve NetSupport bağlantıları kuruldu

ZARARLI BULAŞAN IP:172.16.4.205
MAC ADRES:00:59:07:b0:63:a4
HOSTNAME: Rotterdam-pc
ŞİRKET DOMAIN:mind-hammer.net
İŞLETİM SİSTEMİ: Windows 7 (NT 6.1)

DETAYLI ANALİZ

19 temmuz 2019-18:52 tarihinde 172.16.4.205 cihazı "mysocalledchaos.com" adlı zararlı web sitesini ziyaret etti ve SocGholish JavaScript Web Inject saldırısına maruz kaldı. JavaScript kodu, kurbanın tarayıcısına enjekte edilerek zararlı yazılımın indirilmesine neden oldu.Kurban makine 81.4.122.101 ve 93.95.100.178 adreslerinden Lets Encrypt Free SSL sertifikası kullanan kötü amaçlı sunucularla bağlantı kurdu.Muhtemel bir RAT veya zararlı payload indirildi.
Son olarak 15:01-16:47 saatleri arası http://31.7.62.214/fakeurl.htm adresine veri akatarımı gerçekleşmiştir.

TEHLİKE GÖSTERGELERİ

-mysocalledchaos.com-166.62.111.64
-http://31.7.62.214/fakeurl.htm
-81.4122.101
-93.95.100.178
-185.243.115.84