PCAP Analiz

Hasan Karaca

14.03.2025

1- Zararlı bulaşmış olan PC’nin IP adres, MAC adres ve hostname bilgilerini ?

IP adres : 172.16.4.205

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

Hostname : Rotterdam-pc

2 - Zararlı bulaşmış olan PC’nin User Account bilgisi nedir ?

Matthijs.devries

3 - Zararlı bulaşan şirket ve domain bilgisini yazınız

Domain Adı: mind-hammer.net

Zararlı bulaşan şirket : Mind-Hammer

4 - Zararlı bulaşan windows sürümünü ve zararlı türünü (atak vektörü) yazınız.

windows sürümü : Windows 7 (Windows NT 6.1), 64-bit sürüm

Zararlı türü : SocGholish JavaScript Web Inject (sosyal mühendislik saldırısı**)**

Olay/Vaka raporu:

Olay/Vaka Özeti:

19 Temmuz 2019'da, 18:52-18:57 UTC arasında, 172.16.4.205 IP adresine yönelik şüpheli etkinlikler tespit edildi. 166.62.111.64 IP adresi, kötü amaçlı bir JavaScript dosyası gönderdi. Ardından, 81.4.122.101 ve 93.95.100.178 IP adreslerinden şüpheli SSL istekleri yapıldı. 185.243.115.84 IP adresine kötü amaçlı bir POST isteği gönderildi. Ayrıca, uzak erişim için NetSupport Remote Admin yazılımı kullanıldı.

DETAYLI ANALİZ:

19 Temmuz 2019'da, 18:52 ile 18:57 UTC arasında, 172.16.4.205 IP adresine (MAC adresi: 00:59:07:b0:63:a4) yönelik bir dizi şüpheli etkinlik gözlemlendi. İlk olarak, 166.62.111.64 IP adresinden, SocGholish adı verilen bir sosyal mühendislik saldırısının parçası olarak kötü amaçlı bir JavaScript dosyası gönderildi. Ardından, 81.4.122.101 ve 93.95.100.178 IP adreslerinden gelen HTTPS istekleri dikkat çekti. Bu istekler, Lets Encrypt SSL sertifikalarının kullanıldığı, ancak zararlı olabilecek bağlantıları işaret ediyordu. Bunun hemen ardından, 172.16.4.205'ten 185.243.115.84 IP adresine yönelik .gif dosyasına veri gönderimi ve POST istekleri yapıldı ve kötü amaçlı yazılım yüklendi. 18:57 UTC civarında,

olağandışı bir HTTP isteği farklı bir port üzerinden yapıldı. Aynı zamanda, NetSupport Remote Admin yazılımı kullanılarak uzak erişim sağlandı.

TEHLİKE GÖSTERGELERİ (IOC'LER)

166.62.111.64: SocGholish saldırısının kaynağı.

81.4.122.101: Zararlı SSL sertifikası ve SocGholish yönlendirmesi için kullanılan IP.

93.95.100.178: Zararlı SSL sertifikası ve SocGholish yönlendirmesi için kullanılan IP.

185.243.115.84: .gif dosyasına veri gönderimi ve kötü amaçlı yazılım yüklemesi için hedef IP.

31.7.62.214: Olağandışı HTTP istekleri ve NetSupport Remote Admin için kullanılan IP.