OLAY ANALİZ RAPORU

Hazırlayan: Esra Akteke

Tarih: 15.03.2025

Olay/Vaka

19 Temmuz 2019'da ROTTERDAM-PC isimli bilgisayar, kötü amaçlı bir yazılımın hedefi olmuştur. matthijs.devries adlı kullanıcı, sahte bir tarayıcı güncelleme sayfası aracılığıyla zararlı bir JavaScript dosyasını çalıştırarak sistemini enfekte etmiştir. Bu saldırı SocGholish (FakeUpdates) kampanyasının bir parçası olup enfeksiyon sonucunda NetSupport Manager RAT sisteme bulaşmıştır.

Enfekte Olan Sistem Hakkında Bilgiler

IP Adresi: 172.16.4.205
MAC Adresi: 00:59:07:b0:63:a4
Hostname: ROTTERDAM-PC
Username: matthijs.devries
Bulaşan Zararlı Yazılım: NetSupport Manager RAT
Domain Adı: mind-hammer.net
Dosya Türü: JavaScript (.js)

Saldırının Başlangıcı

Saldırı kullanıcının sahte bir tarayıcı güncelleme bildirimi almasıyla başlıyor. Kullanıcı güvenilir sandığı bu bildirime tıklayarak zararlı bir JavaScript (.js) dosyasını çalıştırıyor. Kayıtlardaki ETPRO CURRENT_EVENTS SocEng/Gholish JS Web Inject Inbound uyarısı bunun SocGholish saldırı kampanyasının bir parçası olduğunu ortaya koyuyor. İlk zararlı trafik 166.62.111.64 IP adresinden 172.16.4.205 hedef sistemine yönlendirilmiş durumda.

Zararlı Yazılımın Sunucularla İletişimi

Enfekte olan sistem, saldırganların kontrolündeki uzak sunuculara HTTPS bağlantıları başlatıyor (81.4.122.101 → 172.16.4.205 ve 93.95.100.178 → 172.16.4.205).
Bu aşamada zararlı yazılım kötü amaçlı dosyaları almak için şifrelenmiş bağlantılar kullanıyor. Saldırganlar, Let's Encrypt gibi yasal SSL sertifikalarıyla zararlı trafiği kamufle ederek güvenlik sistemlerinin şüphelenmesini zorlaştırıyor.

Veri Sızdırma ve Zararlı Trafik

Bulaşan sistem 185.243.115.84 IP adresi ile iletişim kurarak GIF uzantılı dosyalar üzerinden veri gönderiyor. Bu yöntem saldırganların veriyi tespit edilmeden sızdırabilmesi için sıkça kullandığı tekniklerden biri diyebiliriz. "ET POLICY Data POST to an image file (gif)" ve "ETPRO TROJAN POST to a gif file" kayıtları, saldırganların ekran görüntüsü gibi hassas verileri bu yolla elde edebileceğine işaret ediyor.

Zararlı Yazılımın Faaliyete Geçmesi

Bulaşan sistem 31.7.62.214 IP adresi ile HTTP POST istekleri göndererek saldırganın altyapısıyla doğrudan iletişime geçiyor. "ETPRO CURRENT_EVENTS JS.SocGholish POST Request" kaydı sistemin zararlı komutları almakta olduğunu gösterirken, "ET POLICY HTTP Request on Unusual Port Possibly Hostile" uyarısı, bu trafiğin sıradışıportlar üzerinden gerçekleştiğini ve saldırganın güvenlik önlemlerini atlatmaya çalıştığını anlatıyor diyebiliriz.

NetSupport Manager RAT'ın Yüklenmesi ve Uzaktan Erişim

Son aşamada bulaşan sistem 31.7.62.214 adresine NetSupport Manager RAT yazılımını yükleyerek saldırganın uzaktan erişim sağlamasına izin veriyor. "ETPRO POLICY NetSupport Remote Admin Checkin" kaydı bu zararlı yazılımın başarılı şekilde kurulduğunu ve saldırganın kontrolü ele geçirdiğini doğruluyor. "ETPRO POLICY NetSupport Remote Admin Response" uyarısı ise saldırganın artık sistem üzerinde tam erişime sahip olduğunu gösteriyor.

TEHLİKE GÖSTERGELERİ (IOC'LER)

Şüpheli IP’ler

185.243.115.84
31.7.62.213
93.95.100.178

Detaylı analiz sağlandığında Empty.gif dosyasına sık sık yapılan POST istekleri anormal görünüyor. HTTP akışını takip edildiğinde 185.243.115.84 b569023.green.mattingsolutions.co adresine yönlendirildiği görüntüleniyor, kontrol ettiğimde bu adres bazı güvenlik firmaları tarafından zararlı olarak işaretlenmiştir.

Yanıltıcı bağlantı sayfası 93.95.100.178 IP adresi ve ball.dardavies.com alan adı üzerinden Gittiği için şüpheli olarak eklenmiştir.