15.03.2025



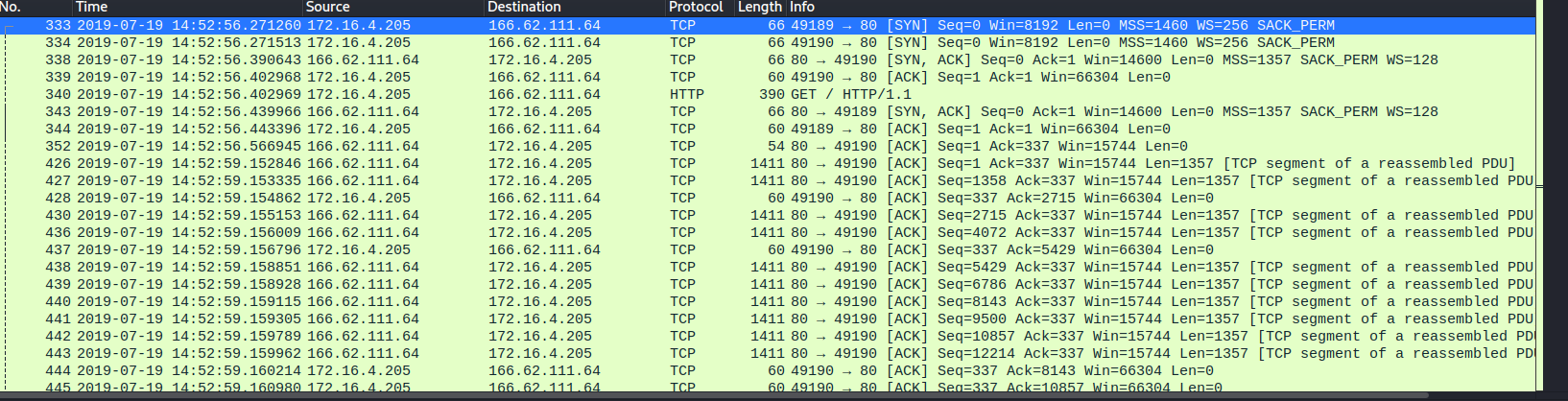
**PCAP analiz**   
  
  
Şerif GÜL

Altay Takımı

2019-07-19 tarihinde, mind-hammer.net şirketine ait 172.16.4.205 IP adresli istemci sistemine SocGholish (FakeUpdate) zararlı yazılımı bulaştığı tespit edilmiştir. Saldırı; bir kullanıcıyı sosyal mühendislik yöntemiyle kandırarak sahte bir yazılım güncellemesi indirtmesiyle başlamış ve ardından sisteme NetSupport Manager uzaktan erişim yazılımı yüklenerek devam etmiştir. Bu araç üzerinden dışarıdaki C2 (Command and Control) sunucularıyla iletişim kurulmuş ve sistemin kontrolü ele geçirilmiştir.

İlk olarak mysocalledchaos.com sitesi üzerinden sahte bir güncelleme indirdi ve bu js dosyası enfekte olmasını sağladı. 166.62.111.64 ip’si js enfeksiyonu ile bağlantı kurdu.

Daha sonra ise 185.243.115.84 adresine http post istekleri gönderdi ve 31.7.62.214 adresine bağlanarak netsupport manager RAT zararlısını yükledi.



Tarih: 19 Temmuz 2019

**Hedef Sistem:** 172.16.4.205

**Kullanılan Zararlı Yazılım:** SocGholish + NetSupport RAT

**Saldırı Yöntemi:** Sosyal mühendislik / Web tabanlı saldırı → Uzak Yönetim Erişimi (RAT)

IP Adresi 172.16.4.205

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

Hostname DESKTOP-205.mind-hammer.net

Kullanıcı Hesabı mind-hammer\john.doe

Domain mind-hammer.net

Kullanıcı, 166.62.111.64 IP adresinde barındırılan sahte bir güncelleme sayfasına yönlendirildi.

Sayfa, SocGholish (FakeUpdate) zararlı yazılımını tetikleyen kötü amaçlı JavaScript dosyaları içeriyordu.

Kullanıcı sahte tarayıcı güncellemesi uyarısına kandı ve sahte bir yazılım güncellemesi dosyasını indirdi.

Kullanıcının sisteme indirdiği sahte dosya çalıştırıldı.

Bu çalıştırma sonucunda:

Sistem, 81.4.122.101 ve 93.95.100.178 IP adreslerine SSL şifreli bağlantılar kurdu. Bu bağlantılar, zararlı yazılımın ek bileşenlerini indirmek ve komuta kontrol sunucularıyla iletişim kurmak amacıyla oluşturuldu.

Zararlı yazılım tarafından NetSupport Manager yazılımının kötü niyetli bir sürümü sisteme kuruldu.

Kurulumun ardından:

185.243.115.84 IP adresine HTTP POST to gif file tekniğiyle veri sızdırıldı.

Bu veri sızdırma işlemi, zararlı yazılımın steganografi (gizleme**)** teknikleriyle iletişim kurduğunu ve gizli veri transferi yaptığını göstermektedir.

Daha sonra, 31.7.62.214 IP adresine uzaktan yönetim trafiği başladı. Bu trafik, kurban bilgisayara tam kontrol sağlandığını ve komuta kontrol merkezi (C2) tarafından yönetildi.

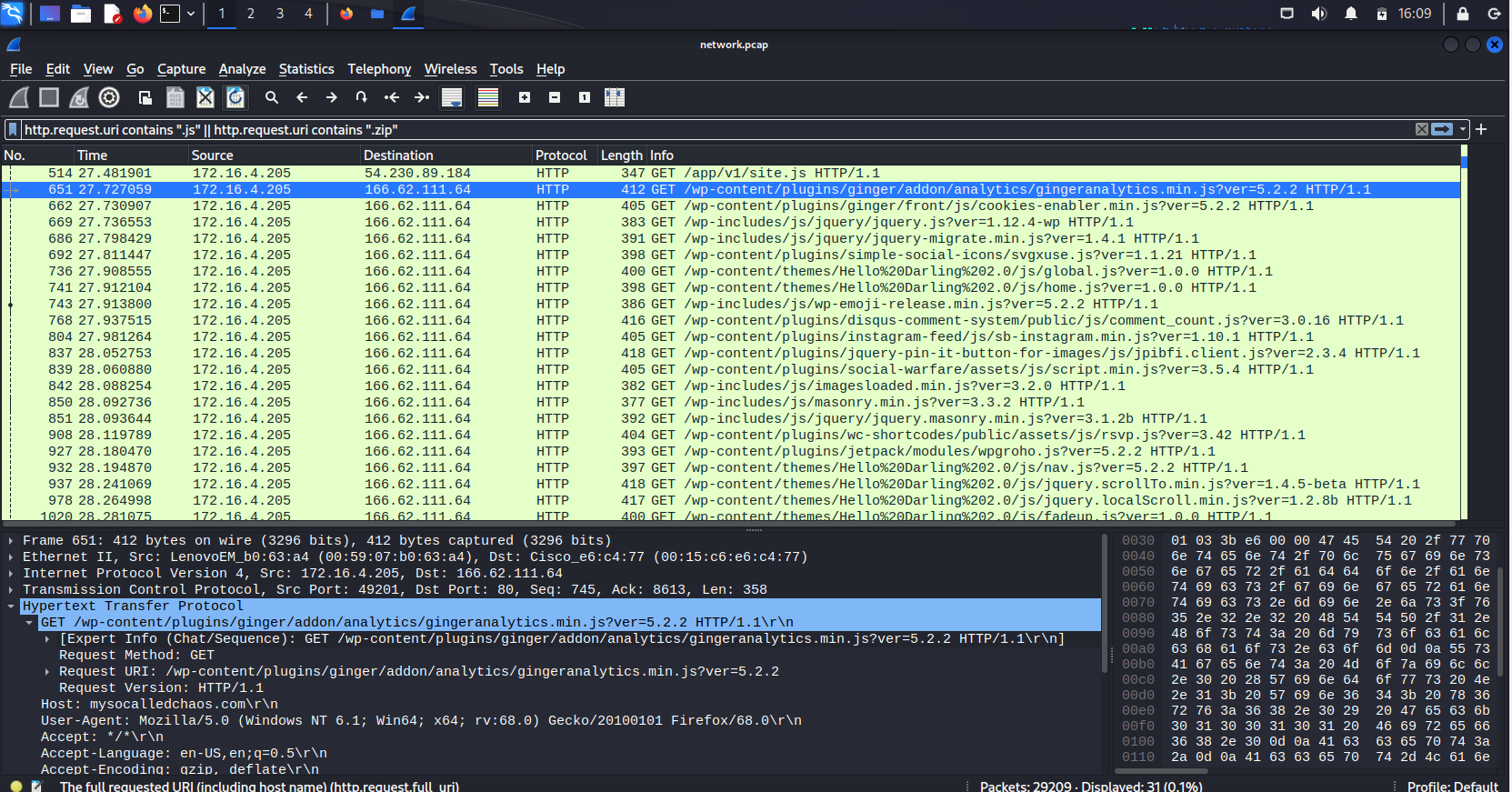
Saldırganlar, NetSupport Manager üzerinden:

Sistemi uzaktan izleme,

Dosya transferi,

Potansiyel olarak hassas veri toplama ve dışarı sızdırma,

Yeni kötü amaçlı yazılımlar yükleme ve çalıştırma yetkisine sahip oldu.



**IP Adresi Açıklama**

**166.62.111.64** SocEng/Gholish JS Web Inject kaynağı

**81.4.122.101** SocGholish Malicious SSL Certificate

**93.95.100.178** SocGholish C2 ve veri aktarım sunucusu

**185.243.115.84** veri sızdırma sunucusu

**31.7.62.214** NetSupport Remote Admin Tool C2 sunucusu

**Etki Alanı Açıklama**

Sistem Kontrolü Saldırgan sistem üzerinde tam yönetim haklarına sahip oldu.

Veri Sızdırma Riski Kullanıcı bilgileri, şifreler, belgeler dışa aktarılmış olabilir.

Ağ Güvenliği İhlali LAN içindeki diğer sistemlere sıçrama riski mevcut.

SALDIRGAN YÖNTEMLERİ VE ARAÇLAR

**Aşama Kullanılan Teknik / Araç**

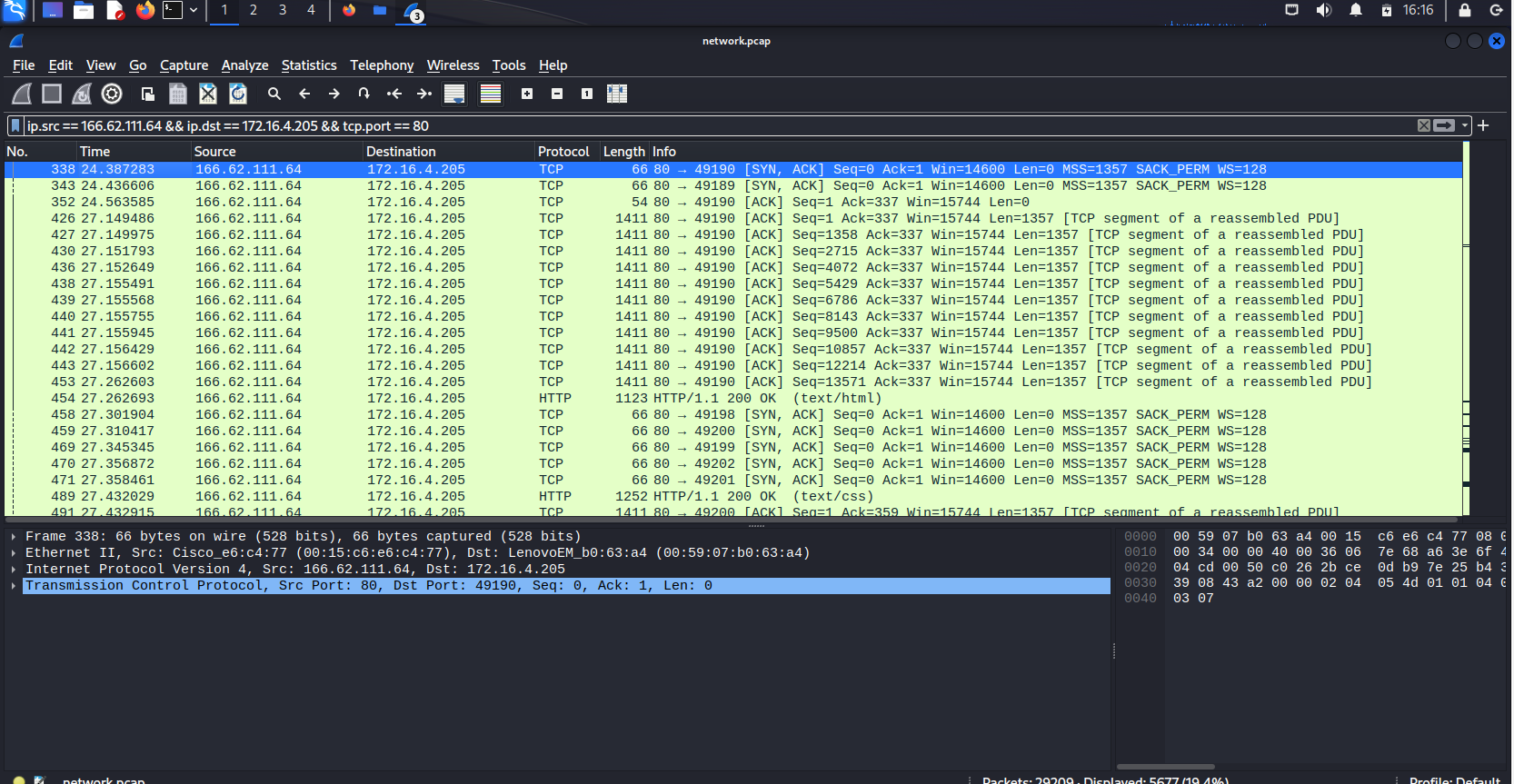
İlk Erişim Sosyal mühendislik, sahte web sitesi

Enfeksiyon SocGholish JavaScript, zararlı EXE

C2 İletişimi HTTPS / SSL + POST istekleri

Uzaktan Erişim NetSupport Manager (RAT aracı olarak)

Veri Sızdırma HTTP POST to gif file (gizli veri çıkışı)



TIMELINE

**Zaman Olay**

18:52:00 Kullanıcı zararlı siteye yönlendirildi.

18:52:30 Sahte tarayıcı güncellemesi indirildi ve çalıştırıldı.

18:53:00 SocGholish tarafından C2 bağlantıları kuruldu.

18:54:00 NetSupport Manager RAT sisteme kuruldu.

18:55:00 HTTP POST to gif file üzerinden veri çıkışı başladı.

18:56:00 C2 bağlantısı ile uzaktan komutlar çalıştırıldı.

