PCAP DOSYASI ANALİZİ

Hazırlayan: Şevval Kömeç

Tarih: 14.03.2025

1. OLAY/VAKA ÖZETİ

Tarih/Zaman: 19 Temmuz 2019, 18:53 - 22:05
Etkilenen IP: 172.16.4.205
Saldırı Tipi: SocGholish Malware Enfeksiyonu, Veri Sızdırma, Kötü Amaçlı SSL Sertifikaları, Uzaktan Yönetim Aracı Kötüye Kullanımı (NetSupport)
Özet:
Şirket ağına bağlı 172.16.4.205 IP adresine sahip Rotterdam-PC adlı cihazın, kötü amaçlı bir web sitesinden SocGholish adlı zararlı yazılımın indirilmiş olduğu belirlenmiştir. Bu süreçte sahte Let's Encrypt SSL sertifikalarının kullanıldığı ve güvenilmeyen bağlantıların yapıldığı tespit edilmiştir. Ayrıca şüpheli POST istekleriyle veri sızdırıldığı görülmüştür.
Saldırgan tarafından, NetSupport uzaktan yönetim aracı kullanılarak sistemin kontrol altına alınmaya çalışıldığı anlaşılmıştır.

2. DETAYLI ANALİZ

Zararlı Bulaşmış Cihazın Bilgileri

IP Adresi: 172.16.4.205
MAC Adresi: 00:59:07:b0:63:a4
Hostname: Rotterdam-PC
Kullanıcı Hesabı: Belirlenememiştir (Ancak işletim sisteminin MSFT 5.0 - Windows olduğu görülmüştür).
Şirket Adı: Mind-Hammer
Domain: mind-hammer.net
İşletim Sistemi: Windows (MSFT 5.0, muhtemelen Windows 10 veya Windows Server olduğu değerlendirilmiştir).
Saldırı Vektörü:
Saldırının, kötü amaçlı bir web sitesine (SocGholish ile ilişkili) erişim sağlanmasıyla başladığı anlaşılmıştır.
Ball.dardavies.com ve mysocalledchaos.com gibi şüpheli sitelere GET isteklerinin gönderildiği tespit edilmiştir.
Bu sitelerden zararlı JavaScript kodunun indirilmiş olabileceği düşünülmektedir.

Cihazın, sahte SSL sertifikaları üzerinden kötü amaçlı bağlantılar kurduğu belirlenmiştir.
ball.dardavies.com sitesine TLSv1.2 şifreleme ile güvenilmeyen SSL bağlantıları yapıldığı görülmüştür.
Kullanılan SSL sertifikasının TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 olduğu tespit edilmiştir.

Cihazın, kötü amaçlı bir GIF dosyasına veri sızdırdığı tespit edilmiştir.
b5689023.green.mattingsolutions.co adresine empty.gif dosyasının POST edildiği belirlenmiştir.
Bu, saldırgan tarafından SocGholish zararlısının kullanılarak çalınan bilgilerin bir GIF dosyası gibi gizlenmiş olduğu ihtimalini göstermektedir.

Saldırganın, NetSupport üzerinden kontrol sağlamaya çalıştığı belirlenmiştir.
31.7.62.214 adresine fakeurl.htm adlı sahte bir web sayfası üzerinden POST isteği yapıldığı

görülmüştür.
Bu durumun, NetSupport'un kötüye kullanıldığına ve saldırganın cihazı uzaktan yönetmeye çalıştığına işaret ettiği değerlendirilmiştir.

Ağ içi hareketlilik gösteren diğer şüpheli IP'ler tespit edilmiştir:
195.171.92.116 → geo.netsupportsoftware.com
Saldırganlar NetSupport kullanarak kurban makineyi uzaktan yönetebilir ve ağdaki diğer cihazlara yayılabilirler.

3. IOC'LER

Şüpheli IP Adresleri ve Alan Adları

166.62.111.64 → mysocalledchaos.com (Kötü amaçlı JavaScript içerdiği değerlendirilmiştir).
93.95.100.178 → ball.dardavies.com (Sahte SSL bağlantısı içerdiği tespit edilmiştir).
185.243.115.84 → b5689023.green.mattingsolutions.co (Veri sızdırma amacıyla kullanıldığı anlaşılmıştır).
31.7.62.214 → fakeurl.htm (NetSupport üzerinden saldırganın yönetim sağlamaya çalıştığı belirlenmiştir).
195.171.92.116 → geo.netsupportsoftware.com (NetSupport kötüye kullanımıyla ilişkili olduğu tespit edilmiştir).

Şüpheli Ağ Trafiği

ETPRO CURRENT_EVENTS SocEng/Gholish JS Web Inject → Zararlı JavaScript saldırısının tespit edildiği belirlenmiştir.
ETPRO TROJAN Observed Malicious SSL Cert (SocGholish Redirect) → Sahte SSL sertifikalarının kullanıldığı anlaşılmıştır.
ET POLICY Lets Encrypt Free SSL Cert Observed → Şüpheli SSL bağlantılarının yapıldığı belirlenmiştir.
ETPRO POLICY NetSupport Remote Admin Checkin & Response → Saldırgan tarafından NetSupport'un kötü amaçlı kullanımına yönelik girişimlerin yapıldığı görülmüştür.

Kötü Amaçlı POST & Veri Sızdırma

http://b5689023.green.mattingsolutions.co/empty.gif
Çalınan verilerin GIF formatında gizlenerek gönderildiği anlaşılmıştır.
http://31.7.62.214/fakeurl.htm
Saldırganın, NetSupport üzerinden cihazı ele geçirmeye çalıştığı web sayfası olduğu belirlenmiştir.

SONUÇ VE YAPILMASI GEREKENLER

1. Etkilenen Cihazın İzole Edilmesi

172.16.4.205 (Rotterdam-PC) IP adresine sahip cihazın acilen ağdan izole edilmesi gerektiği değerlendirilmiştir.

Cihazın tamamen temizlenmesi ve yeniden güvenli bir şekilde yapılandırılması gerektiği belirtilmiştir.

2. Ağdaki Tüm Cihazların Taranması

Ağdaki diğer cihazların NetSupport ve SocGholish zararlısı için taranması gerektiği önerilmiştir.
Active Directory ortamında bilinmeyen hesaplar veya şüpheli girişler olup olmadığı incelenmelidir.

3. Güvenlik Önlemleri

Ağ güvenlik politikalarının güncellenerek şüpheli SSL sertifikalarının engellenmesi gerektiği belirlenmiştir.
NetSupport ve benzeri uzak yönetim araçlarının erişiminin kısıtlanması önerilmiştir.
Firewall ve IDS kurallarına aşağıdaki şüpheli IP'lerin eklenmesi gerektiği belirtilmiştir:

- 166.62.111.64
- 93.95.100.178
- 185.243.115.84
- 31.7.62.214
- 195.171.92.116