

GoPhish Platformu ile Kurumsal Oltalama (Phishing) Simülasyonu ve Senaryo Analizi

Konu: E-posta Sosyal Mühendislik Testi & Kimlik Avı Simülasyonu

Araçlar: GoPhish Framework, SMTP Sandbox (Email Sandbox)

Hedef Kurum (Simüle): Nexora Bulut Teknolojileri A.Ş.

Tarih: 25 Ağustos 2026

Özet: Bu makale/doküman, kurum içi siber güvenlik farkındalığını artırmak amacıyla **GoPhish** açık kaynaklı sosyal mühendislik platformu kullanılarak gerçekleştirilen uçtan uca bir oltalama (phishing) simülasyonunu detaylandırmaktadır. Senaryo kapsamında "Nexora Bulut Teknolojileri A.Ş." altyapısı hedef gösterilerek "Olağandışı Giriş Denemesi" temalı sahte bir e-posta ve ona bağlı zararlı/sahte kimlik doğrulama portalı tasarlanmıştır. Çalışmada kullanılan vektörler, teknik mimari, kullanıcı psikolojisini hedef alan unsurlar ve savunma mekanizmaları adli bilişim standartlarına uygun şekilde incelenmiştir.

1. Giriş ve Amaç

Günümüz siber tehdit aktörlerinin kurumsal ağlara sızmak için en sık başvurduğu yöntemlerin başında Sosyal Mühendislik ve Oltalama (Phishing) saldırıları gelmektedir. Teknik güvenlik önlemlerinin (Güvenlik Duvarı, E-posta Filtreleri, IDS/IPS vb.) gelişmesiyle birlikte saldırganlar doğrudan insan faktörünü ve kullanıcı zafiyetlerini hedef almaktadır.

Bu çalışmanın temel amacı; kurumsal e-posta kullanıcılarının şüpheli e-postaları tespit etme yetkinliğini ölçmek, "Nexora Bulut" ortamı taklit edilerek hazırlanan bir senaryoda kimlik bilgileri (credential harvesting) avcılığının aşamalarını ve risklerini teknik olarak belgelemektir.

2. Test Mimarisi ve Kullanılan Araçlar

Simülasyonun güvenli bir ortamda yürütülmesi ve gerçek kullanıcı trafiğini aksatmaması adına isolated (izole) lab mimarisi kurulmuştur:

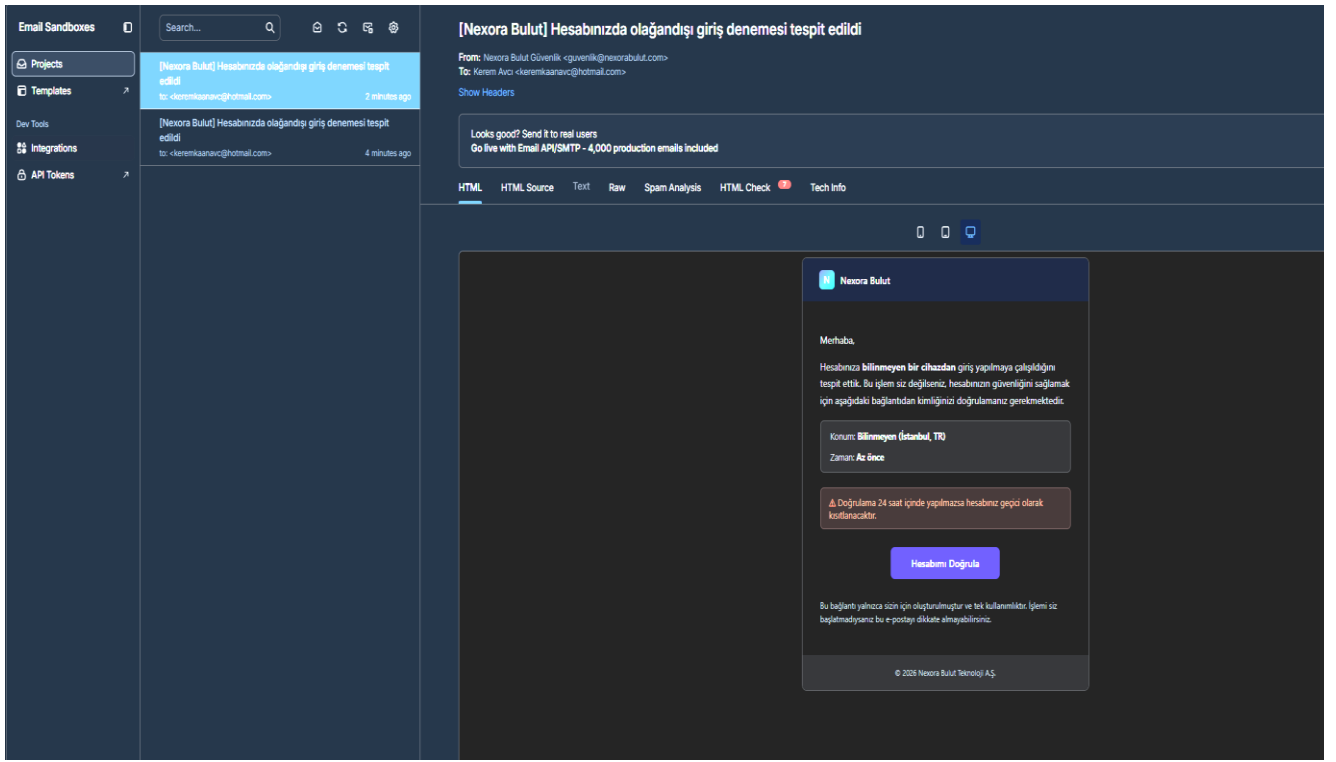
Bileşen	Kullanılan Araç / Teknoloji	İşlev ve Açıklama
Simülasyon Motoru	GoPhish Phishing Framework	Şablon yönetimi, hedef liste tanımlama, e-posta gönderimi ve istatistik takibi.
E-posta İletimi (SMTP)	Email Sandboxes / Mailtrap / GoPhish Profile	Güvenli mail gönderimi ve test sunucu entegrasyonu.
Hedef Senaryo Markası	Nexora Bulut Güvenlik (Sahte Kurum)	Kullanıcının güvendiği kurumsal servis sağlayıcı rolü.
Landing Page (Giriş)	Özel HTML/CSS Sahte Portal	Giriş bilgilerini (E-posta ve Şifre) yakalamak üzere tasarlanan sahte arayüz.

3. Ortalama Senaryosu ve Teknik Detaylar

3.1. E-posta Yemi Tasarımı (Phishing Template)

Saldırı simülasyonunda kullanıcı üzerinde aciliyet ve korku hissi uyandırarak mantıksal sorgulamayı devre dışı bırakmak amaçlanmıştır.

- **Gönderen Adı/Adresi:** Nexora Bulut Güvenlik <guvenlik@nexorabulut.com>
- **Konu:** [Nexora Bulut] Hesabınızda olağandışı giriş denemesi tespit edildi
- **İçerik Stratejisi:** Kullanıcıya hesabına bilinenin dışında bir konumdan (Bilinmeyen - İstanbul, TR) erişilmeye çalışıldığı bildirilir.
- **Aciliyet Unsuru:** "Doğrulama 24 saat içinde yapılmazsa hesaba erişim geçici olarak kısıtlanacaktır." uyarısı eklenmiştir.
- **Eylem Çağrısı (CTA):** Mantıksal yönlendirme için öne çıkan mor renkte "Hesabımı Doğrula" butonu konumlandırılmıştır.

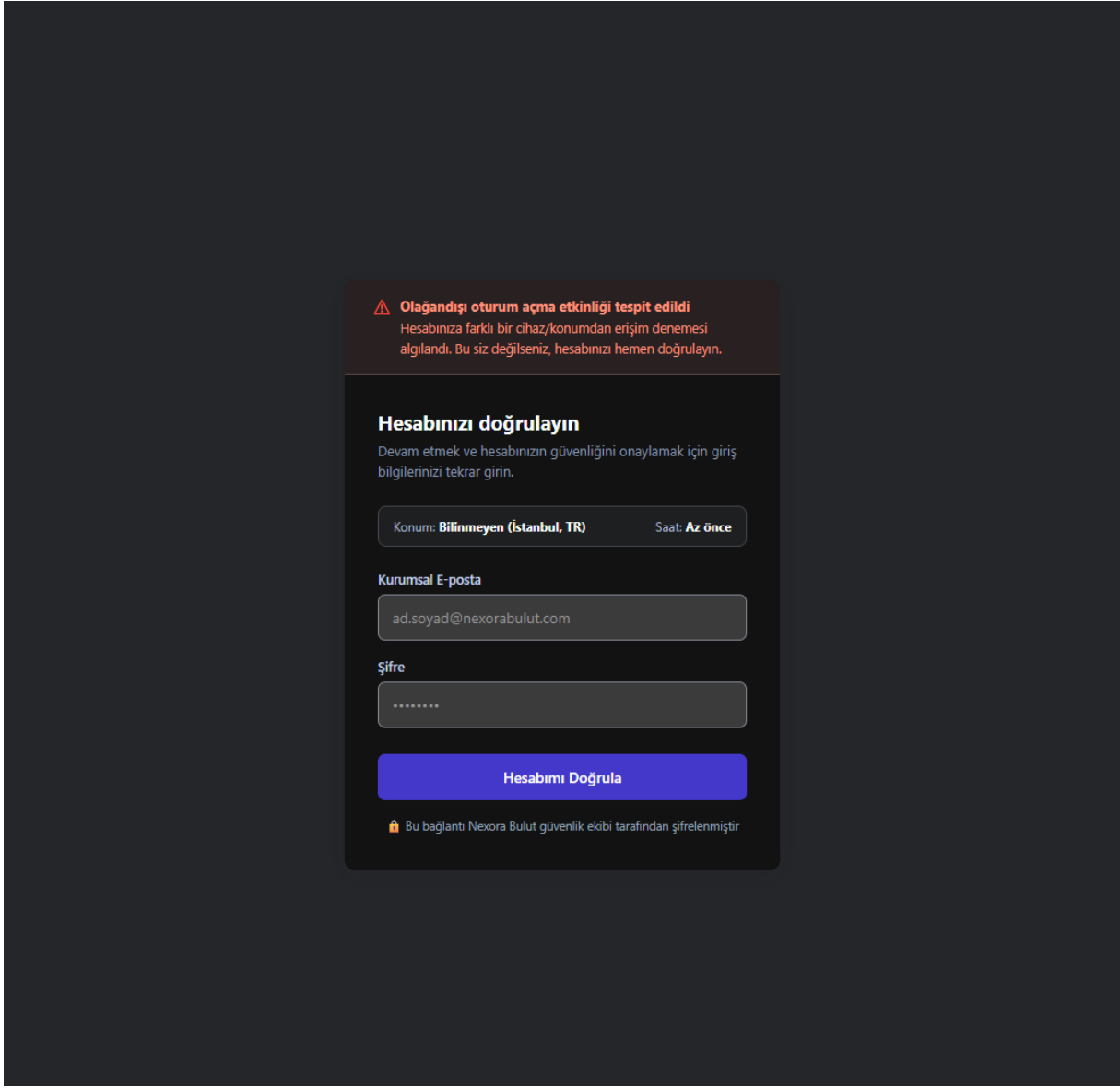


Sosyal Mühendislik Vektörü: Saldırganlar sıklıkla "Güvenlik Bildirimi" maskesi arkasına saklanır. Kullanıcı, hesabını koruma içgüdüleriyle hareket ederken bağlantının gerçek alan adını (Domain) kontrol etmeyi göz ardı eder.

3.2. Sahte Giriş Sayfası Tasarımı (Landing Page & Credential Harvesting)

Gelen e-postadaki yönlendirme bağlantısına tıklayan kullanıcı, modern koyu tema (dark mode) tasarımıyla hazırlanmış son derece inandırıcı bir giriş doğrulama portalına aktarılır.

- **Görsel Tasarım:** Nexora Bulut markasının logosu, renk paleti ve tipografisi birebir taklit edilmiştir.
- **Giriş Formu Alanları:**
 - **Kurumsal E-posta** (Yer tutucu: ad.soyad@nexorabulut.com)
 - **Şifre** (Gizli veri alanı)
- **Güven Hissi Verici Elemanlar:** Alt kısma yerleştirilen "🔒 Bu bağlantı Nexora Bulut güvenlik ekibi tarafından şifrelenmiştir" ibaresi ile sahte bir güvenlik algısı pekiştirilmiştir.



4. Adli Bilişim ve İnceleme Göstergeleri (IoC - Indicators of Compromise)

Yapılan bu simülasyonda bir güvenlik analisti veya adli bilişim uzmanı açısından tespit edilmesi gereken temel göstergeler şunlardır:

İnceleme Noktası	Gerçek Durum / Zafiyet Göstergesi
E-posta Üstbilgileri (Headers)	Gönderici adresi (nexorabulut.com) ile mailin geldiği gerçek SMTP sunucusu ve IP adresi uyumsuzdur. SPF, DKIM ve DMARC doğrulamaları başarısız olacaktır.
Bağlantı URL Adresi	"Hesabımı Doğrula" butonunun yönlendirdiği domain, kurumun resmi domaini değil, GoPhish listener IP/domain adresidir.
Veri Girişi Takibi	Form gönderildiğinde HTTP POST isteği GoPhish sunucusuna düşmekte ve girilen parolalar veritabanına kayıt edilmektedir (Simülasyon modunda şifreler hash'lenmeli veya maskelenmelidir).

Güvenlik Uyarısı: Gerçek hayat simülasyonlarında açık metin (clear-text) parolanın kaydedilmesi KVKK ve bilgi güvenliği standartlarına aykırıdır. GoPhish konfigürasyonunda "Capture Submitted Passwords" seçeneği kapalı tutulmalı veya yalnızca parolanın girildiği an (event) loglanmalıdır.

5. Önleme ve Kurumsal Koruma Önerileri

1. Teknik Önlemler:

- **SPF, DKIM ve DMARC Politikaları:** E-posta alan adının taklit edilmesini engellemek için Strict DMARC politikaları (`p=reject`) uygulanmalıdır.
- **E-posta Güvenlik Ağ Geçidi (SEG / FortiMail vb.):** Gelen e-postaların başlık bilgileri ve içerisindeki URL'ler dinamik tarama (URL rewriting/sandbox) aşamasından geçirilmelidir.
- **Çok Faktörlü Kimlik Doğrulama (MFA / 2FA):** Kullanıcı şifresini sahte sayfaya kaptırsa dahi TOTP / FIDO2 güvenlik anahtarları sayesinde hesabın ele geçirilmesi engellenmelidir.

2. İnsan ve Farkındalık Önlemleri:

- Kullanıcılara e-postalarda gelen butonların arkasındaki gerçek URL adreslerini kontrol etme alışkanlığı (Hover over link) kazandırılmalıdır.
- Olağandışı aciliyet bildiren e-posta geldikten sonra ilgili kuruma farklı bir kanaldan (telefon, dahili hat) teyit mekanizması kurulmalıdır.

6. Sonuç

Gerçekleştirilen bu GoPhish ortalama simülasyonu, kurumsal kimlik taklidinin ve sosyal mühendislik senaryolarının ne kadar ikna edici olabileceğini kanıtlamaktadır. Kullanıcının tek bir tıklama ile sahte oturum açma arayüzüne yönlendirilmesi ve parolasını teslim etme riski, sürekli farkındalık eğitimlerinin ve çok katmanlı güvenlik (Defense-in-Depth) yaklaşımının önemini bir kez daha ortaya koymaktadır.