Dupli Checker

PLAGIARISM SCAN REPORT

0%
Plagiarised

100%
Unique

Date	2021-05-13
Words	682
Characters	6252

Content Checked For Plagiarism

ŞİFRE ÇALMA ve PHİSHİNG

İÇİNDEKİLER

GİRİŞ

Bilişim teknolojileri, çoğu alanda hayatlarımızı kolaylaştırdığı gibi bunun yanında güvenlik konusunda yeni açık ve kaygıların oluşmasını sağlamıştır. Artık internet dünyasındaki suç türleri günümüz dünyamızda fiziksel olarak yapılan suç türlerinden daha fazlalaşmış ve isim olarak İngilizceden devşirme olan bu kelimeler çoğu kişide anlama zorluğu çektirmiştir. Bu nedenle kendisine yapılan suçun ne olduğunu bilmeyen kişi hakkını aramada da eksiklik yaşamaktadır. Bu konularda şifre çalma konusunda belli yöntemler vardır. Bu yöntemlerden mağdur olmamak için bu yöntemleri bilmek gerekmektedir. Bu saldırılar özel olarak araç gereç gerektirmedikleri için günlük hayatta en çok kullanılan sistemlerdir. Bu yapılan saldırılar şahsa, kurum yöneticileri, devlet yöneticilerine veya herhangi bir kişiye yapılabilmektedir.

Şifre Çalma Yöntemleri Nelerdir?

Şifre çalma yöntemleri olarak genel olarak kullanılan 3 yöntem mevcuttur. Bunlar Phising, Brute Force, Keylogger vardır.

Phishing:

Phishing İngilizce' de Password (şifre) ve fishing (sazan avı) kelimelerinin birleşmesiyle oluşmuştur. Phishing internet dünyasının en etkili ve en eski saldırılarının başındadır. Phishing genel anlamda kişilerin e-posta adreslerine cezbedici sahte içerikler iletilerek parola, kimlik bilgisi veya özel bilgileri çalınmaya çalışılır.

Brute Force:

Bu yöntemin Türkçe karşılığı kaba kuvvet saldırısı olarak adlandırılmaktadır. Adı üzerine ham güç kullanılmaktadır. Kişinin şifresini bulana dek art arda şifre deneme işlemi gerçekleştirilmesine Kaba Kuvvet Saldırısı denmektedir. Hangi kişinin şifresini çalmak istenirse o kişinin adı soyadı anne adı baba adı doğun tarihi vb. bilgiler ile çeşitli kişiye özel wordlist hazırlama programlarıyla kapsamlı şifre listesi oluşturulur ve seçilen şifre deneme programı ile ilgili hesaba denenir ve şifre bulunduğunda şifre deneme işlemi sonlandırılır.

Keylogger:

Bu sistem için öncelikle şifresini istediğiniz kişinin cihazına casus yazılım yüklenmesi gerekmektedir. Bu işlemi yaptıktan sonra keylogger programı herhangi bir harfe dokunulduğunda bu harfleri kaydederek size veri olarak gönderir. Bu veriler içinde tarama yapılarak şifre bulunur.

Phishing Nasıl Yapılır?

Oltalama(phishing) bireylere ve bazen de şirketlere karşı yapılmaktadır. Bu saldırılarda sahte e-posta ve web sayfaları kullanılmaktadır. Bu sahte e-posta ve web sayfaları üzerinden hesap bilgileri, kredi kartı, değerli bilgiler ve vb. bilgi çalınmaya çalışılmaktadır. Bu işlemi yaparken bağınız iletişiminiz olan kurummuş gibi kişinin ismi geçecek şekilde e-posta gönderilir. Alt kısımda da web sayfası verilir. Bu önceden hazırlanmış olan sahte siteye giren kullanıcı bilgilerini girip sayfaya girmeye çalıştığında gerçek sayfaya yönlendirilir ve bilgileri site tarafından kaydedilmektedir. Bu bilgilerle kötü niyetli kişiler kullanıcıları maddi, manevi zarara uğratmaktadır. Bu sistemin diğer bölümü ise sahte çekiliş web siteleri oluşturmaktır. Burada belli çekiliş vaatleri verilir. Bunu gören kullanıcı bu çekilişe katılmak ister. Tabi bu çekilişe katılmak için kişinin kişisel bilgileri istenir. Kullanıcıda verilen vaatteki kazanmak için bu bilgileri girdiğinde kötü niyetli kişiler bunları kullanarak yine kişilere zarar vermektedir.

Phishing' ten Nasıl Korunulur?

Oltalama yöntemi genel olarak aynı olsada senaryolar hepsinde değişmektedir. Bu konuda önemli olan saldırılar konusunda bilinçli olmaktır. Bazı dikkat edilmesi gereken konular vardır Bunlar şunlardır:

Dil kullanımı: Oltalama saldırılarında gönderilen maillerde yazım kurallarına çok dikkat edilmez. Şirketler buna dikkat etmektedir. Fakat oltalamayı yapan kişi maili gerçek kurum mailini kopyalayarak yaptıysa dil kullanımına bakılması bir işe yaramayacaktır. Dil kullanımında diğer dikkat edilmesi gereken konu ise tehditvari kelimeler kullanılmasıdır. Mesela "24 saat içinde gerekli işlem yapılması gerekir.", "Gerekenler yapılmadığı durumunda hesabınız bloke olacaktır" ve vb. ifadeler mevcutsa oltalama olması büyük ihtimaldir.

Kullanılan Site Linkleri: Öncelikle kurumlar e-posta göndererek hesabınıza giriş yapılmasını istemez. Fakat şifre değiştirme hesabın dondurulması veya farklı senaryolarla bu e-postalara kanılabilmektedir. Bu mailin gerçek kurum tarafından gönderildiğini gönderdiğini öğrenmek için şu hususa da dikkat edilmesi gerekmektedir. Maillerde kullanıcıları yönlendirilen sitedeki linki gerçek siteye benzerlikte linkleri kullanılır. Bu yüzden bu linklerin kontrolünün yapılması gerekmektedir. Örnek: Gerçek site: www.instagram.com Kopyalanmış site: www.instegram.com bu çok ufak ve dikkat edilmeyen ayrıntı kişilerinin mağduriyet yaşamamasına sebep olmaktadır.

Web sitesinde bir diğer bakacağımız konu ise site başında "https" olmasıdır. Bu ibare sitenin sertifikaya sahip olduğunu gösterir.

Son Olarak:

- Herhangi bilginin girilmesi istenen veya belli dosyaların indirilmesi gerektiğini söyleyen e-postalara temkinli yaklaşılmalıdır.
- Maillerde karşı tarafın kullandığı dile dikkat edilmelidir.
- Web sitelerinin URL adreslerine dikkat edilmelidir.

KAYNAKÇA:

Bilgi Teknolojileri Müdürlüğü (2018), Phising Nedir? Nasıl Farkedilir? Antalya Bilim Üniversitesi, https://antalya.edu.tr/tr/bolumler/bilgi-sistemleri-mudurlugu/icerik/bilgi-guvenligi/phishing-nedir-nasil-farkedilir

BilişimTeknolojileri ve Siber Güvenlik Derneği, Phishing Saldırısı Nedir? Nasıl Korunulur? https://antalya.edu.tr/tr/bolumler/bilgi-sistemleri-mudurlugu/icerik/bilgi-guvenligi/phishing-nedir-nasil-farkedilir