forbiap

Your partner today, for tomorrow's technology

FİDYE YAZILIMI NEDİR?

Bilgisayar ve bilgisayarın erişebildiği dosyaları şifreleyerek, kullanıcıların dosyaları kullanmalarını engellemek üzere kurgulanmış bir zararlı yazılımdır.

Bu zararlı fidye yazılımdan etkilenmiş ortamlarda bir bilgi dokümanı yerleştirilir ve bu bilgi dokümanında dosyaları eski haline getirilmesi için gereksinimlerden ve talimatlar yer alır. Gereksinimlerin en başında fidye talep edilir. Fidyenin ödenme ortamı kripto paralar üzerinden gerçekleşmesi istenir. Böylelikle kime fidye verildiği öğrenilmemektedir.

FİDYE YAZILIMI NASIL BULAŞIR?

Yaygın olan yöntem sahte ortamlardan sahte içerikler ile mail ortamında kullanıcıların merak duygusunu ön plana çıkarak içerikler ile hata yapması sağlanıyor. Fatura, kargo, uçak bilgileri gibi içerikler ve ünlü firmaların görsel olarak kopyalayarak kullanıcılarda güven duygusunu oluşturuluyor. Kullanıcılarda sağlanan merak ve güven duygusu ile bilgisayarına indirdikleri uygulamayı çalıştırmalarıyla birlikte verileri şifreleniyor.

Diğer bir yayın olan yöntem ise uzak bağlantısı direkt erişime açık sunuculara yapılan Brute-Force ataklar sonucunda kullanıcıların parolaları ele geçiliyor. Böylelikle yetkili kullanıcı ile giriş yapıldıktan sonra fidye yazılımı çalıştırılmaktadır.

FİDYE YAZILIMINDAN NASIL KORUNUZ?

1 – Antivirüs ve Anti-Spam Sistemi

Bilgisayar ve sunucularda güncel bir anti-virüs sistemi kullanılmalıdır. Kullanılan anti-virüs günlük olarak kontrol edilmeli ve anti-virüs motorunun güncel ve sağlıklı çalıştığından emin olunmalıdır.
Mail akışı düzenli olarak takip edilmeli ve doğru kurallar ile kullanıcılara sahte maillerin gelmesi engellemelidir.

2 – Yedekleme Sistemi

Kullanıcıların çalıştıkları ve kullandıkları verilerin ortak bir alanda saklanması sağlanıp, bu alanın düzenli zaman aralıklarında yedeklemeleri sağlanmalıdır. Yedek dosyalarında farklı bir veri merkezi veya varsa kuruma ait başka lokasyonda kopyaları saklanmalıdır.

3 – Kullanıcı doğrulama Sistemi

Ofis dışında çalışan fakat ofisteki sunucu ortamına uzaktan bağlanıp çalışan kullanıcılar için bağlantılarını gerçekleştirirken kimlikleri teyit edilmelidir. Kimlikleri teyit edilen kullanıcıların parolaları zayıf olsa dahi telefonlarına gelen tek kullanımlık parolalar ile sisteme erişimleri daha güvenli olacaktır.

4 – Güvenlik duvarı Sistemi

Bilgisayar ve sunuculara gelecek uzakta bağlantı taleplerini doğru yönlendirmek, özel sanal ağlar oluşturmak, iç ve dış ağ arasındaki trafik için doğru kurallar oluşturulmalıdır.

5 – Personel Eğitimi

Sahte hesaplar ve sahte mail örnekleri personellere gösterilmeli ve farkındalık eğitimleri düzenlenmelidir. Basit düzeyde mail analiz işlemleri aktarılmalıdır.

FORBIAP Bilişim Teknolojileri
Çağlayan Mahallesi, Maya Sokağı, No: 13/3 Kağıthane, Istanbul/TR
0850 840 0 456
www.forbiap.com
info@forbiap.com