T.C. Sağlık Bakanlığı

Sağlık Bilgi Sistemleri
Genel Müdürlüğü

Siber Olaylara Müdahale (SOME) Birimi

Güvenli E-Posta Kullanımı
Ve
Oltalama Saldırılarına Karşı Önlemler

KASIM 2016

İçindekiler

1. E-Postalarınız Neden Tehlikede?

Teknoloji ile gelişen iletişim ağları saldırganları da geliştirerek normal kullanıcılara daha da yakınlaştırmıştır. Günümüzde kurumların ve kişilerin en önemli bilgileri, dokümanları E-Posta hesapları üzerinde akmaktadır.

Örneğin; Kurumunuzun satın alma bilgileri, çalışanların sicil bilgileri vs…

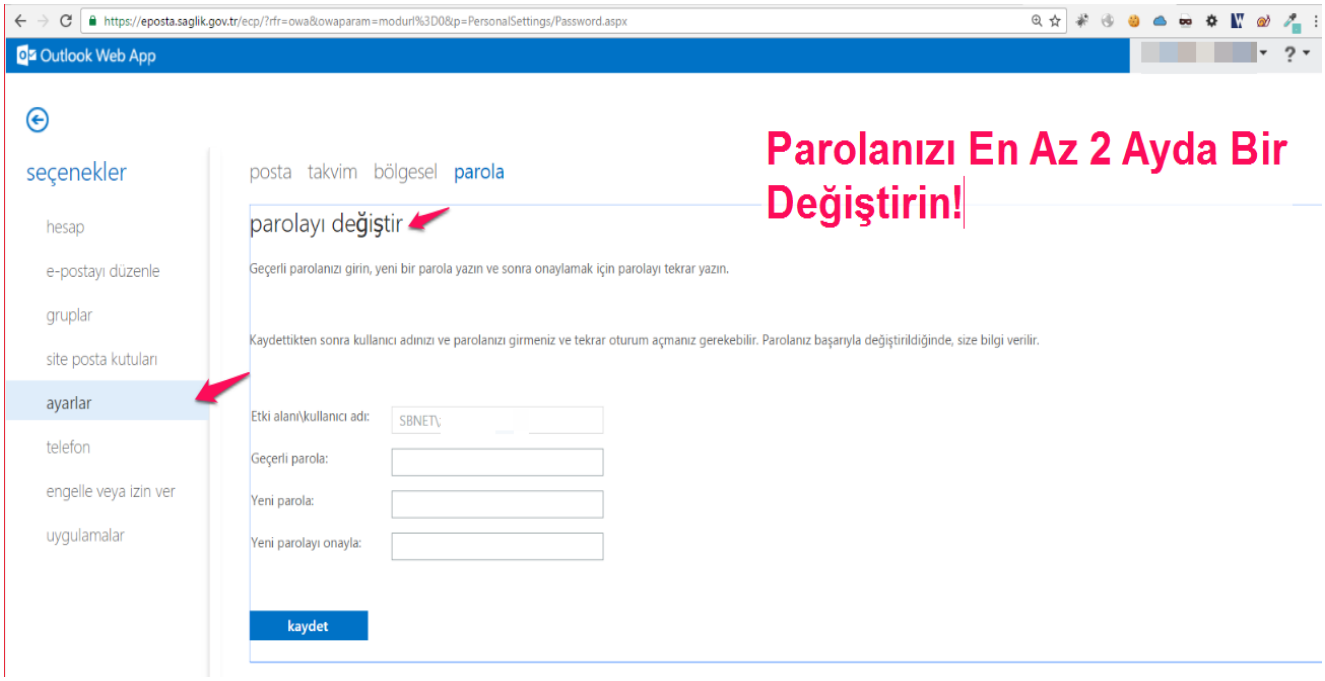
Kurumların ve kişilerin bilgilerini çalmak için düzenlenen sosyal mühendislik saldırılarının bir çok çeşidi vardır. Ancak E-Postalar üzerinden olan saldırılar oltalama (Phishing) saldırıları olarak adlandırılır.

2. Oltalama (Phishing) Saldırısı Nedir?

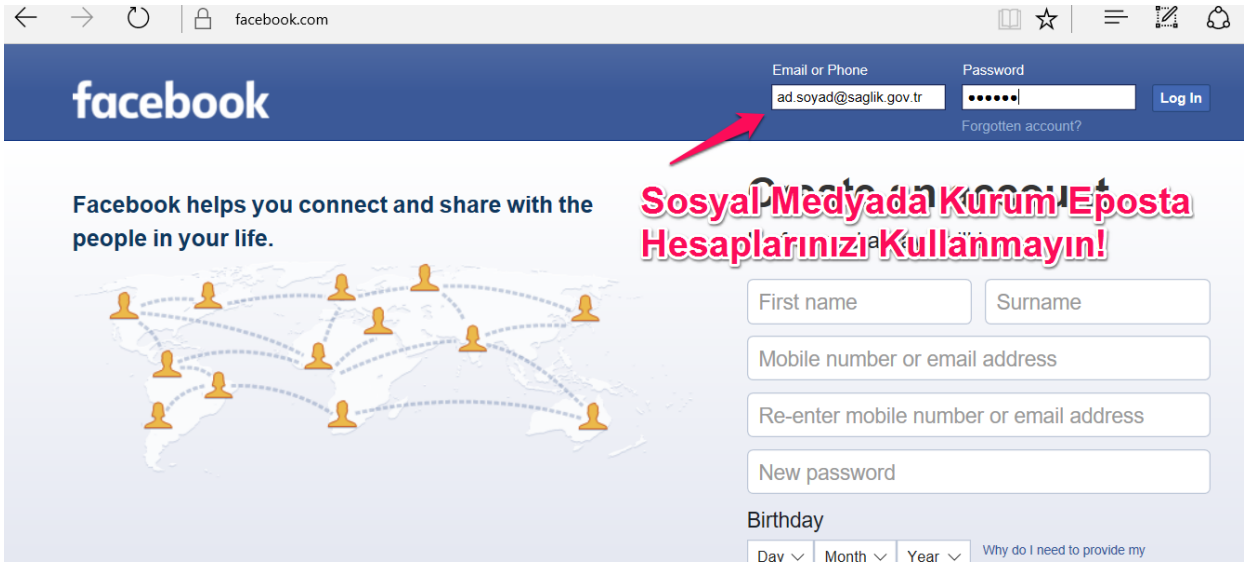
Saldırgan kullanıcılara zararlı içerikler barındıran epostalar aracılığıyla ulaşır. Bu zararlı içerikler kimi zaman tıklanan linkler kimi zaman ekteki resim, PDF veya excel gibi dosyalardır. Kullanıcı saldırganın gönderdiği linke tıkladığında veya eklentiyi indirip açtığında tüm bilgisayarının kontrolü ele geçirilebilir, hesapları çalınabilir.

3. Oltalama (Phishing) Saldırılarından Korunma Yolları

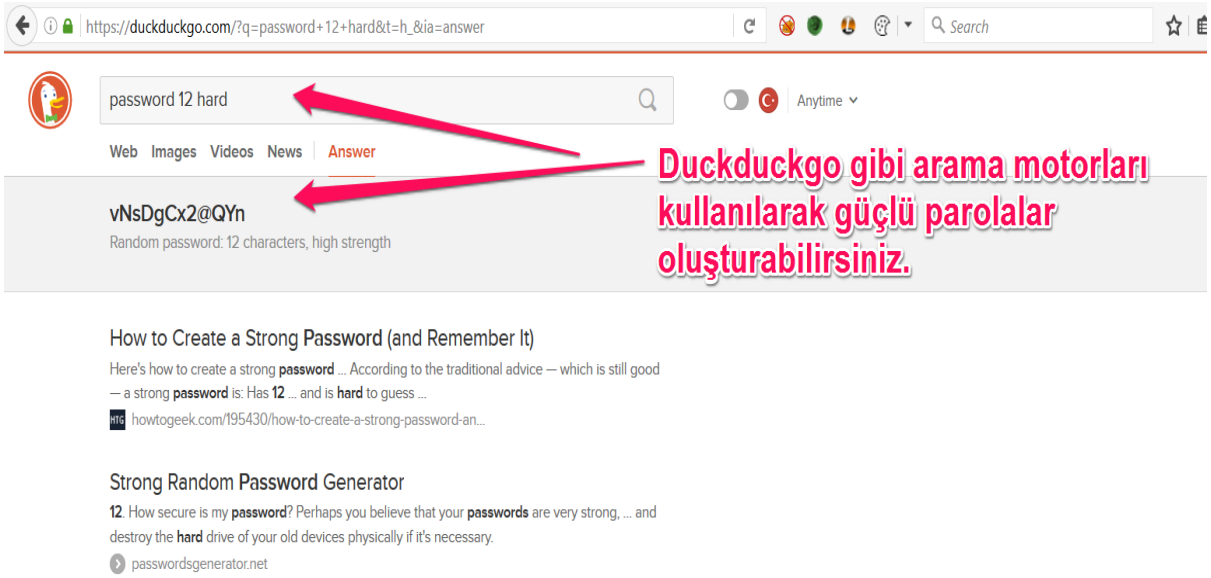
✓ E-Posta hesabınızın parolasını sıklıkla değiştiriniz. (2 ayda bir tavsiye edilmektedir.)



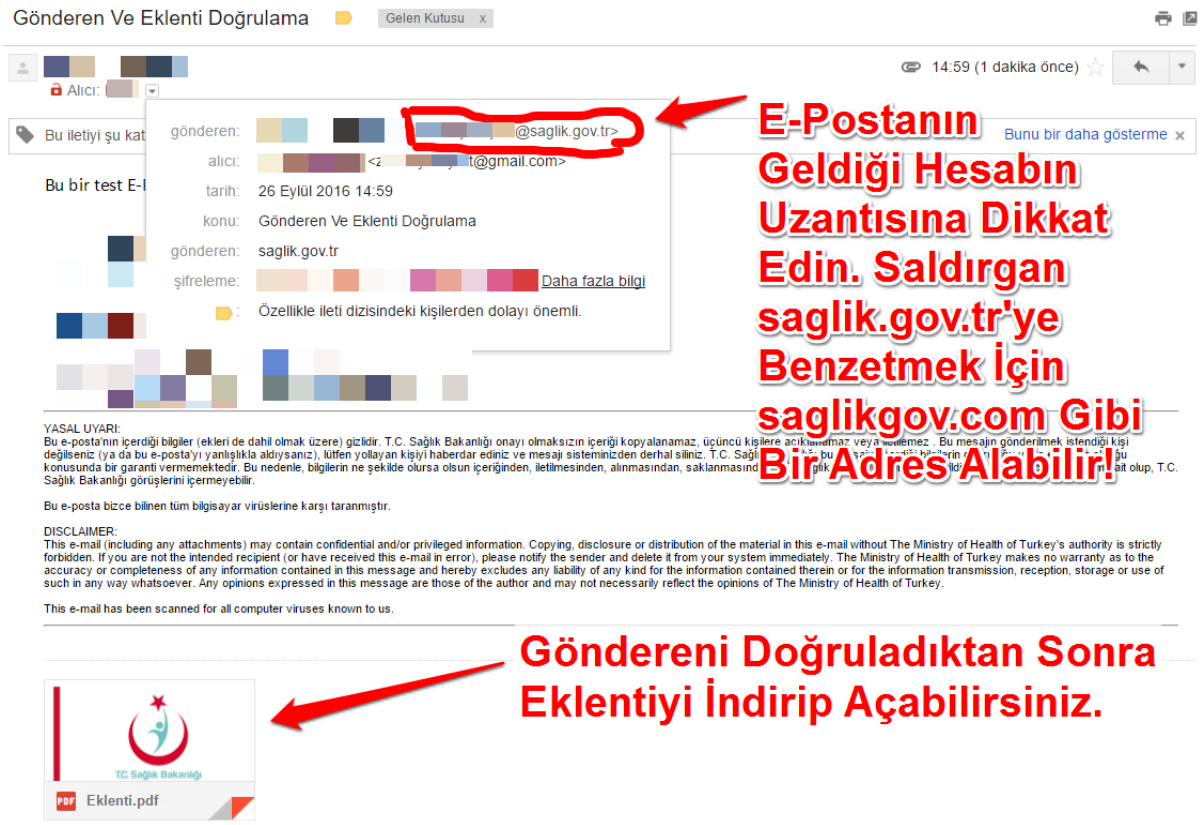
✔ E-Posta hesabınız ve sosyal medya hesaplarınız gibi yerlerde aynı parolaları kullanmayın. Herhangi bir hesabınız çalındığında (hacklendiğinde) diğer hesaplarınızda da benzer parolalar saldırgan tarafından denenecektir.
Örneğin; Facebook, Twitter gibi sosyal medya hesapları ya da online bankacılık uygulamaları



✔ Kırılması zor parolalar kullanınız. Parolanız en az 12 karakter olup içerisinde büyük küçük harf, sayı ve özel karakterler içermeli. Kırılması ne kadar zor ve anlamsız parolalar seçerseniz herhangi bir parola kırma saldırısına karşı daha güvende olursunuz.
NOT: Parola Güvenliği hakkında; Bilgi Güvenliği Politikaları Kılavuzundaki C.5 Parola Güvenliği başlıklı maddeleri takip edebilirsiniz...!!!



✓ Gelen her eklentinin açılmaması konusunda hassas davranınız. Öncelikle epostayı gönderen kişiden emin olun. Gönderenin eposta adresini ayrıntısını görerek dikkatlice inceleyin. Gerçekten o kişinin adresi olduğundan emin olun.



ÖNEMLİ !!!

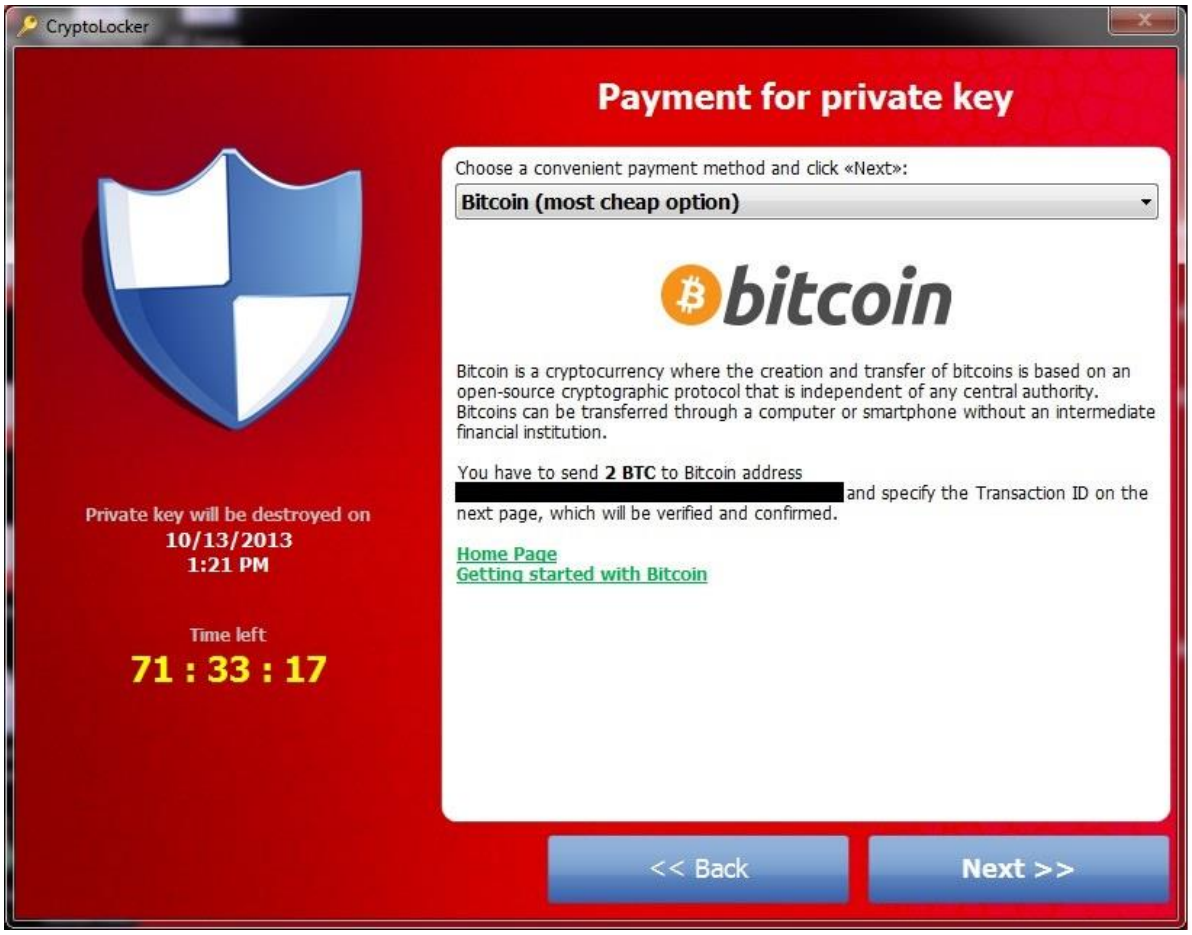
Son zamanlarda **Ransomware** yani **veri fidyeciliği** için gönderilen zararlı e-posta oranında büyük bir artış bulunmakta. Kesinlikle gelen e-posta'ların eklentilerine ve gönderenine dikkat ediniz. Halk arasında bu saldırının sıkça duyulan ismi "**Cryptolocker**"dır. Ancak Cryptolocker saldırılarında bir çok şifreleme türü vardır. Bir kısmı tekrar deşifre edilebilse de saldırganlar da gün geçtikçe deşifre edilmesi daha zor şifrelemeler ile saldırmaktadır. Bu sebeple kesinlikle e-postalardaki eklentiler indirilirken veya çalıştırılırken, linklere tıklanırken çok dikkatli olunmalıdır. Çünkü devlet kurumları olası saldırı hedefleri arasında listelerde en üst sıralarda bulunmaktadır. Zira kötü niyetli saldırganlar tarafından kamu kurumlarından bir çok gizli ve önemli veri çalınmaya çalışılmaktadır.

Her şeye rağmen bilgisayarınızın masaüstünde aşağıdakilere benzer bir fidye notu bulursanız:

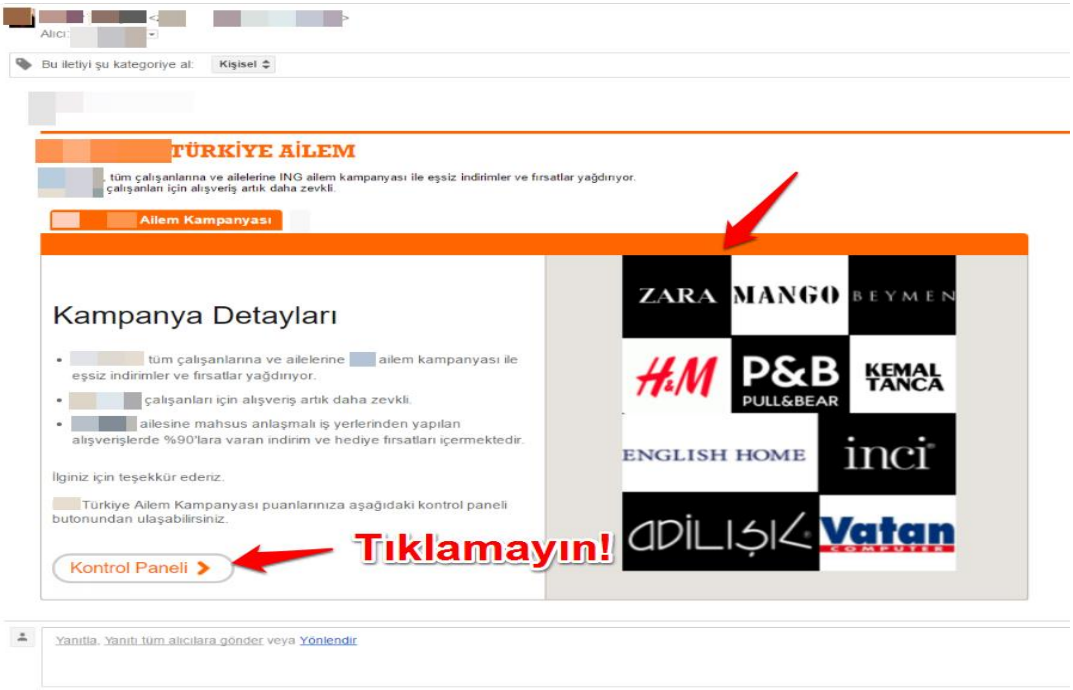
- Bilgisayarınızı hızlıca direkt olarak kapama tuşundan kapatın.
- Kablo ile internete bağlı iseniz kabloyu çıkartın.
- Siber Olaylara Müdahale (SOME) Birimine ivedilikle haber veriniz.

- **NOT:** Yaşanılan bilgi güvenliği ihlallerini https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir sayfasından giriş yaparak Genel Müdürlüğümüze bildiriniz.

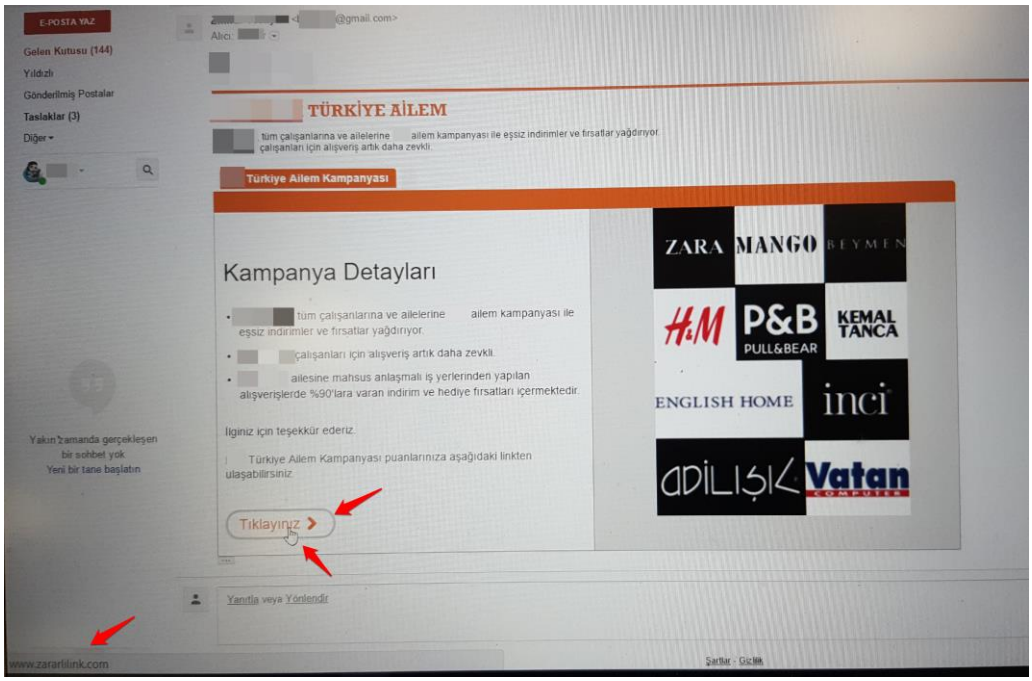
Örnek: Fidye notu ekran görüntüleri:



✓ Mağazalardan gelen indirim kampanyalarını içerdiğini söyleyen E-Postalar içerisindeki linklere E-Postanın gerçekten mağazadan geldiğini doğrulamadan tıklamayınız veya eklentileri indirmeyiniz.



- Farenizi linkin üzerine tıklamadan getirin ve sol altta yanıp sönen link adresini kontrol edin.



- Gelen linklere direkt tıklamak yerine yeni bir tarayıcı sekmesi açıp linkleri adres çubuğuna elle girerekte adres kontrolü yapabilirsiniz.
- Güvenmediğiniz (Kurumsal Olmayan) sitelere E-Posta adresinizi vermeyiniz.
- Herkese açık forumlara web sitelerine kesinlikle E-Posta hesabınızı yazmayınız.
- Gelen Spam maillerde, Spam klasöründe "Unsubscribe" / "Aboneliği İptal Et" kısımlarına tıklamayınız. Bu sadece spam maili gönderen saldırgana E-Posta hesabınızın gerçek olduğu ve kullanıldığı hakkında bildirim gönderir. Daha sonrasında hedefli bir saldırıya maruz kalabilirsiniz.
- Spam E-Postalara cevap vermeye çalışmayın. Cevap verseniz dahi muhtemelen saldırgana ulaşmaz. Çünkü E-Postanın gelen başlığı (FROM Header) bilgisi sahtedir.
- E-Postalarınızda kişisel bilgi göndermemeye özen gösteriniz.
- Parolalarınızı kimseyle paylaşmayınız.
- E-Posta hesabınızdan çıkış yaptığınıza emin olun.
- Kurumsal bir hesaptan gelse bile gönderen kişi veya birim hakkında imzası olmayan E-Postalar konusunda dikkatli olunuz. Gönderenin kimliğini doğrulamaya çalışınız.

Örnek: Kişisel bilgileriniz vb. gibi gizlilik içeren dosyaları parolalı şekilde sıkıştırarak (Winrar, Winzip vb. programlar yardımıyla), parolasını karşıdaki kişiye kısa mesaj ile göndererek e-posta güvenliğini artırabilirsiniz.

✓ Oltalama E-Postalarını tanımayı öğrenelim;

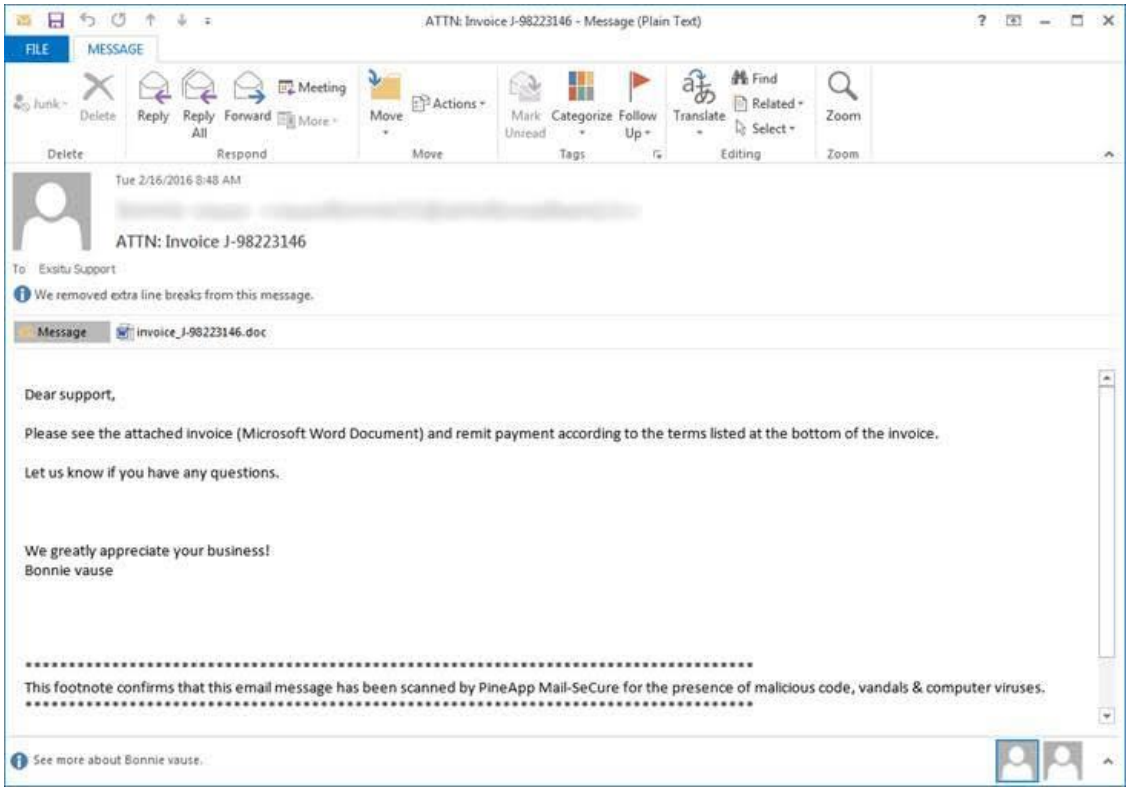
- ❖ E-Posta hesabınızın kapanacağına, borçlanabileceğinize dair uyarı / tehdit içeriyor mu?
- ❖ E-Posta birden kazandığınız indirimler, hediye çekleri gibi şeyler içeriyor mu?
- ❖ Konu kısmında "Acil - Urgent" vb… kelimeler yazan E-Postalara dikkat ediniz. Sırf ilginizi çekmek ve endişelendirmek için saldırgan tarafından yazılmış olabilir.
- ❖ E-Postayı gönderen adresin uzantısı tanımadığınız bir uzantı mı? Sanki çalıştığınız kurumun ya da ilgilendiğiniz mağazaların adlarına benzetilmeye çalışılmış gibi?
- ❖ Gönderilen bilginin sizinle veya kurumunuzla gerçekten ilgisi var mı?

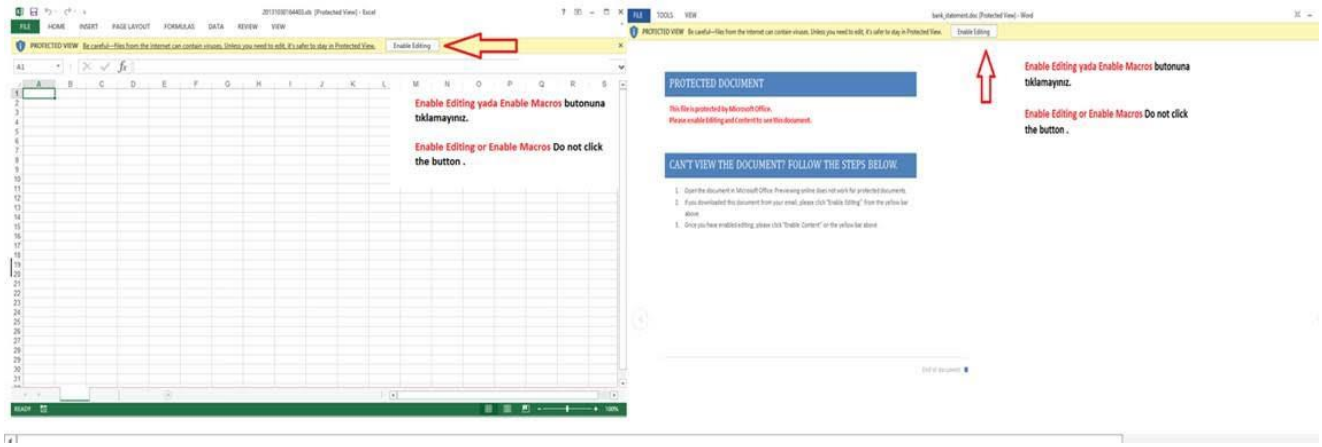
Sistem Yönetimi Daire Başkanlığı / Siber Olaylara Müdahale (**SOME**) Birimi
Yıldızevler Mah. Simon Bolivar Cad. Sedat Simavi Sok. No:36 Kat:2 06550 Çankaya / ANKARA
Tel: +90 (312) 501 20 77 – 20 47 – 20 24
E-Posta : some@saglik.gov.tr
Web Site : https://some.saglik.gov.tr

4. Oltalama (Phishing) E-Posta Örnekleri

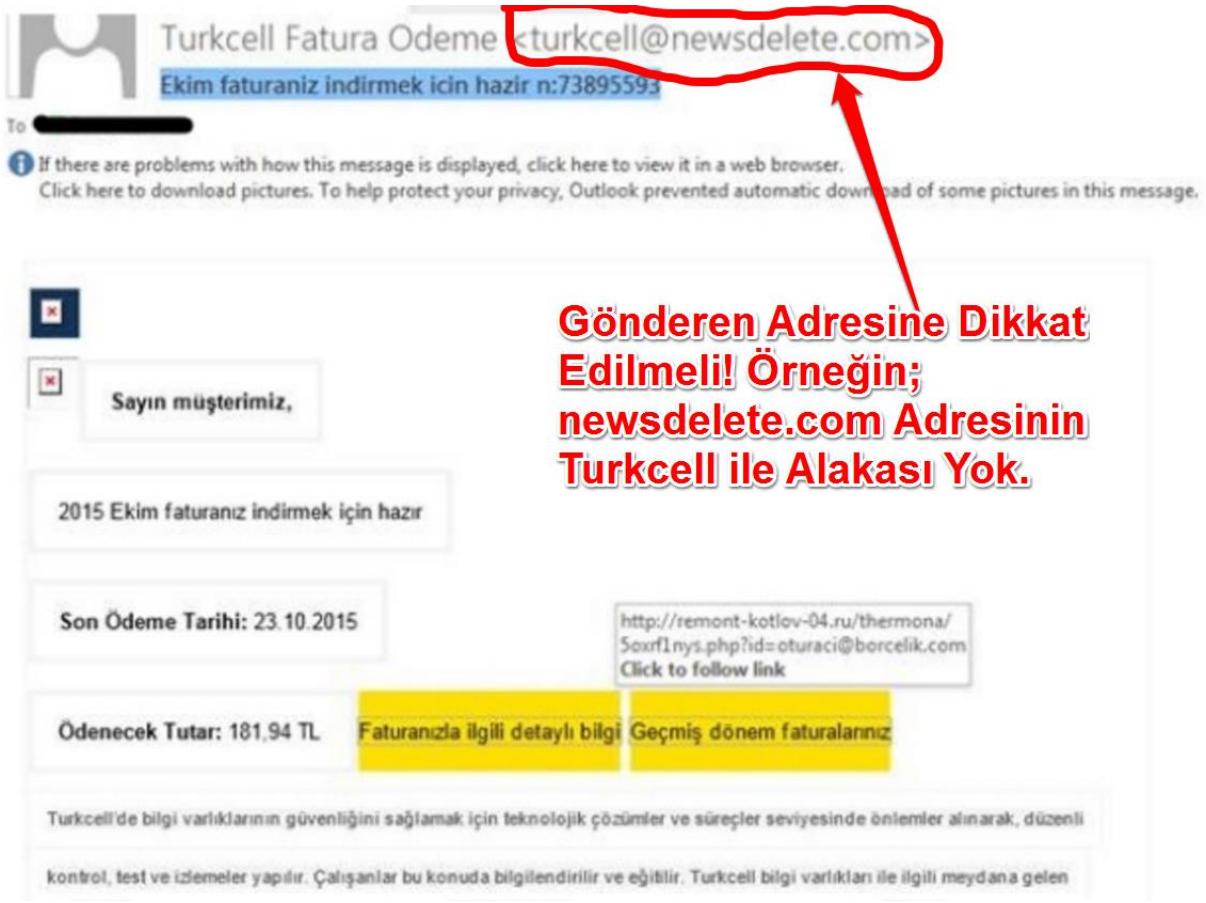
Locky Ransomware Oltalama E-Posta

Aşağıdaki gibi bir mailde gönderilen dosya eki Excel formatındadır. Ve açtığınızda düzenlemeyi etkinleştirmenizi veya Macro'ları etkinleştirmenizi ister. Eğer bunu yaparsanız sisteminizi ele geçirip tüm dosyalarınızı size fidye ödemeye zorlayacak biçimde şifrelenmesine sebep olmuş olursunuz.





Aşağıdaki örnekte Turkcell Fatura Ödeme adresinden geliyormuş gibi gözüken ve "Ekim faturanız indirmek için hazır" başlıklı E-Posta sıkça karşılaşılan saldırı türlerinden biridir. Linke tıklandığında **www.remont-kotlow-04.ru** adresine yönlendiren bir E-Postadır. E-Posta üzerinden yönlendirilen linkelere çok dikkat edilmelidir. Saldırgan örnekteki gibi alakasız bir adrese yönlendirebileceği gibi dikkatsizlik anında gözden kaçabilecek **turkcelll.com** gibi bir adrese yönlendirebilir. Unutulmamalılıdır ki hiç bir kurumsal şirket sayın müşterimiz diyerek başlamaz Sizlere hitap şekli olarak adınız ve soyadınızla bildirime başlar.



5. Adım Adım Oltalama (Phishing)

Aşağıdaki adımlarda kurumsal veya özel e-posta adresinize ulaşan zararlı yazılımların, bilgisayarlarınızda nasıl etkinlik kazandığını, zarar verme yöntemlerini, minimum hasarla kurtulmanın yollarının neler olduğu anlatılmaktadır.

(Buradaki örneklerle E-Posta güvenliği farkındalığını arttırmak amaçlanmıştır.)

Zararlı Yazılımın Etkinlik Kazanma Adımları ve Önleyici Aksiyonlar;

1- Saldırgan avlanmak üzere oltayı internet denizine bırakır.

- Saldırgan gerçeğine çok yakın veya taklit isim kullanan bir internet sitesi tasarlar. Site adı size yabancı gelmez, hatta güvenilir gibi görünebilir.
  Örn: www[.]ttnet-bilgilendirme[.]org
- Asıl amacı bir an önce taklit site veya E - Posta içindeki linke tıklamanızı sağlamak, ardından zararlı yazılımı bilgisayarınızın çalıştırmasını sağlamaktır.
- Ama acele etmez, aynı zamanda güveninizi kazanmayı hedefleyerek kesin olarak zararlı yazılımı indirmenizi ister.

2- Oltaya doğru gelmeniz için yemleme yapar.

- Bu amaçla bir anlık dikkatinizi dağıtacak, merakınızı çekecek türde **"tanıdığınız birinden gelen, ekinde yabancı türde dosya(documents.zip), yüksek meblağ içeren faturalar(TTNET - TELEKOM), kayıp kargonuzun takip fişi(PTT), banka EFT dekontunuz(HSBC), e-devlet uygulamanız vb."** sizin adınızın ve soyadınızın geçtiği ifadeler kullananır.

- "Bu benzerlikte e-posta alırsanız linklere tıklamadan, ekleri açmadan e-postayı incelemek üzere support@xyz adresine iletin ve siliniz. (E-Postanızın **silinmişler** klasöründen de siliniz.)"

3- Avlanmanızın yüksek ihtimal olduğu anlar. (Çok Dikkatli olmanız gereken anlar)

Hergün yüzlerce e-posta okuduğumuzdan ilk bakışta dikkatinizi veremezseniz ayırt edici bazı özellikleri gözden kaçırabilirsiniz.

- Böyle bir e-posta aldığınızda **"Önce, güvenilir kişi veya kurumdan gelen bir e-postamı? şüphesiyle inceleyin."** hiç bir linke tıklamadan ve ekli dosyaları açmadan. Önce bu durumu gözden geçirin.
- Diyelim ki e-posta içinden linke tıkladınız ve bir sayfa açıldı sizden bazı bilgiler girmenizi istiyor, **"Şu anda doğru kurumun internet adresindemisiniz? Dikkatli Olun!!"**
- Saldırganın amacı dikkatinizi dağıtmak ve bir an önce e-posta veya taklit site içindeki linke tıklayıp dosyalarınızı şifreleyecek zararlı yazılımı indirmenizi ve çalıştırmanızı sağlamaya çalışmaktır.
- Sizin gözünüzde güven kazanmak için gerçek internet sitelerinde olan güvenlik doğrulama mekanizmalarını işletiyormuş gibi görünür. (Örn: Karakter veya resim doğrulama adımları)

- Her adımda güveninizi daha fazla kazanır, indirilmesi istenen zararlıdan **hiç süphe etmemeniz amaçlanmıştır.**
- **Unutmayın,** hiçbir kurum sizin bilgilerinizi e-posta ile istemez veya onaylamanızı istemez.

4- Avlandığınızı anladığınızda yaşananlar ve acilen yapmanız gerekenler;

- Eğer bu adıma geldiyseniz ve çalıştırdığınız dosyanın farkında değilseniz, iş amaçlı dosyalarınız, fotoğraflarınız, Dropbox, GoogleDrive, SkyDrive vb. gibi bulut depolüzerindeki dosyalarınız, bilgisayarınızın hızına ve dosyaların sayısına göre ortalama 3 – 8 dk aralığında etkilenebilir.
- Eğer yanlışlıkla linklere tıklar ve dosyaları çalıştırırsanız, bilgisayarınızı normal yollarla kapatmak için zaman kaybetmeyin, mümkün olduğunca hızlı bir şekilde kapatın!!!
- Masaüstü bilgisayar kullanıcıları bilgisayarınızın fişini çekin, Notebook kullanıcıları şarj adaptörünü prizden çekmeli, pili çıkarmalı veya bekleme moduna alıp bilgisayarın çalışmadığından emin olmalıdır.

5- Zararlı Yazılıma Maruz Kalındığında ki Sonuç;

- Ekranınıza saldırgan tarafından düzenlenmiş dosyalarınızın şifresini alabilmeniz için yapmanız gereken ödeme bilgisi gelebilir
- Artık bu aşamada yapılabilecekler çok sınırlıdır. Bu tür zararlılının dosyalarınız üzerinde ki etkisini, problemden önceki haline getirmek neredeyse mümkün olmayabilir.
- Dosyalarınızı kurtarmak için size teklif edilen bedeli saldırgana ödemekle bu siber suçu finanse etmiş olursunuz.
- Ödeme yöntemi ise BITCOIN (internet üzerinde geçerli kabul edilen para birimi) olacagindan ve herhangi bir banka işlemi ile yapamayacağınızdan saldırganı bulmak normal yollarla mümkün olmayabilir.

6- Genel Olarak Kullandığınız Bilgisayarlı Sistemler için Önleyici Tedbirler

- Şüpheli e-posta aldığınızda içindeki linklere tıklamayın, ekindeki dosyayı açmayınız.
- Bilgisayarınızda günlük işleri düşük haklara sahip kullanıcınız ile yapmalısınız*******
- Bilgisayarınızda tarih ve saati değiştirebiliyorsanız, program yükleyebiliyorsanız, zararlı yazılımlarda aynı haklara sahip olur ve bu yetkilerle zarar verir.
- Eğer günlük işlerinizi yaparken daha yüksek haklara ihtiyacınız varsa bilgi işlem birimlerinizden destek isteyebilirsiniz.

Sistem Yönetimi Daire Başkanlığı / Siber Olaylara Müdahale (**SOME**) Birimi **E-Posta :** some@saglik.gov.tr
Yıldızevler Mah. Simon Bolivar Cad. Sedat Simavi Sok. No:36 Kat:2 06550 Çankaya / ANKARA **Web Site :** https://some.saglik.gov.tr
Tel: +90 (312) 501 20 77 – 20 47 – 20 24