CRYPTOLOCKER VİRÜSÜ HAKKINDA BİLGİ NOTU

1. CRYPTOLOCKER VİRÜSÜNÜN TANIMI, YAYILMA/ÇALIŞMA ŞEKLİ VE VERDİĞİ ZARARLAR:

a. CryptoLocker, fidye isteyen kategoride (ransomware) bir zararlı yazılımdır. Türkiye'de son dönemlerde genellikle e-fatura içeren sahte mailler yoluyla yayılmaktadır *(Ancak saldırganların virüsü yayacak yeni yöntemler geliştirebilecekleri unutulmamalıdır, örneğin seçim dönemleri yaklaştığında, Yüksek Seçim Kurulundan gelmiş görüntüsü verdikleri bir sahte e-postada, hangi sandıkta oy kullanılacağına dair bağlantı sunan, aslında bağlantıya tıklandığında virüsün bulaşacağı bir yöntem gibi).*

b. Virüsü yayan siber saldırgan genellikle sahte bir e-fatura dosyası oluşturmakta, fatura tutarını oldukça yüksek göstererek kullanıcının dikkatini çekmekte ve kullanıcıyı gönderdiği maildeki linke *(örneğin "http://efatura.ttnet-fatura.com/" benzeri)* tıklamaya yönlendirmekte, linkten e-faturanın "zip" uzantılı bir dosya halinde indirilmesini sağlamaktadır.

c. Kullanıcı, "*.zip" uzantılı dosyayı açıp içindeki e-fatura dosyasına (*.exe uzantılı) tıkladığında virüs çalışmakta ve kullanıcı bilgisayarındaki tüm dokümanlar (Office dosyaları, resim/video dosyaları, pdf dosyaları vb.) virüs tarafından güçlü şifreleme algoritmaları (AES-256 vb.) ile şifrelenmektedir. Dosyaların uzantıları sonuna ".encrypted", ".sifreli" vb. kelimeler eklenmektedir *(Örneğin; deneme.doc.encrypted)*

ç. Virüs, şifrelediği her bir klasöre ve kullanıcı masaüstüne "SIFRE_COZME_TALIMATI.html" benzeri bir dosya eklemekte ve içeriğinde, *"Uyarı: Tüm dosyalarınız CryptoLocker virüsü tarafından şifrelenmiştir. Bilgisayarınızda ve USB belleklerde olan önemli dosyalarınız, fotoğraflar, videolar ve kişisel bilgiler CryptoLocker virüsü ile şifrelenmiştir. Bizim şifre çözme yazılımını satın almak dosyalarınızı kurtarmak için tek yoldur. Aksi takdirde tüm dosyalarınızı kaybedebilirsiniz."* benzeri bir açıklama ile şifrenin çözülmesi için kullanıcılardan para talep etmektedir. Virüsün bazı türevlerinde ise, aşağıdaki gibi bir uyarı ekranı görünmektedir.

d. Saldırganlar şifrenin çözülebilmesi için kullanıcıları genellikle Bitcoin[1] gibi takibi zor dijital para birimiyle ödeme yapmaya (genellikle 100-300 ABD doları arasında) yönlendirmektedir.

e. Virüs, 2013 yılında ABD'de ortaya çıkmış ve hızla diğer ülkelerdeki bilgisayarlara yayılmıştır. CryptoLocker ve benzer özellikli CryptoWall virüslerinin dünya genelinde 600.000'den fazla bilgisayarı etkilediği ve 5 milyarın üzerinde dosyayı şifrelediği tahmin edilmektedir. Virüsün toplam pay içinde %24 ile en çok ABD'yi etkilediği, ülkemiz için bu oranın yaklaşık %3 olduğu bilinmektedir[2].

f. Virüs, genel çalışma mantığında, zarar vereceği dosyanın şifreli yeni bir kopyasını oluşturmakta, sonrasında orijinal dosyayı silmektedir. Bu silme hızlı silme olabildiği gibi, virüsün bazı türevlerinde güvenli silme şeklinde (en az 3 kez üzerine yazma gibi) de olabilmektedir.

g. Virus, %AppData% klasörüne (C:\Users\KULLANICI ADINIZ\AppData \Roaming) kendini rastgele bir isim ile kurmakta ve bilgisayarın açılışında çalışmak üzere kayıt defterinde (registry) "HKEY_CURRENT_USER\Software\Microsoft\Windows \CurrentVersion\Run" altına, güvenli modda bile çalışabilecek şekilde anahtar oluşturmaktadır. Ayrıca şifrelediği her bir dosya için "HKCU\Software\CryptoLocker\Files" altına bir dosya ismini belirten anahtar değeri eklemektedir.

ğ. Virüsün dosyaları şifrelemesi, dosya sayısına göre saniyeler, dakikalar hatta saatler sürebilen bir işlemdir. Kullanıcı, bilgisayarındaki işlemlerine devam ederken, virüs arka tarafta kullanıcının haberi olmadan dosyaları şifrelemektedir. Virüs şifreleme işlemlerini tamamladıktan sonra kendini kullanıcıya göstermektedir.

h. Kurumlarda, özellikle dosya ve veri tabanı sunucuları ile bilgisayarlarda virüsün şifrelemesi nedeniyle çok ciddi zararlar oluşacağı açıktır. Bunun yanında virüsün şahsi bilgisayarlarda da ciddi kayıplara yol açabileceği göz ardı edilmemelidir. Virüsün dosyalarını şifrelemesi nedeniyle, şahsi bilgisayarlarında uzun süredir yazmakta olduğu kitap çevirilerini, akademik makalelerini, yüksek lisans ve doktora tezleri ile yıllardır biriktirdiği şahsi resim ve video arşivlerini artık açamayan kullanıcılara ait internette birçok haber bulunmaktadır.

2. CRYPTOLOCKER VİRÜSÜNE KARŞI ALINABİLECEK TEDBİRLER VE BULAŞMASI DURUMUNDA YAPILABİLECEK İŞLEMLER:

a. Virüsün dosyaları şifrelemesi durumunda, yapılabilecek çok fazla seçenek bulunmadığından önemli olan husus virüsün bulaşmasını engellemektir. Bu doğrultuda web siteleri veya e-posta üzerinden gelen aldatıcı dosya ve bağlantılara kesinlikle tıklanmamalı ve şu temel hususlar göz önünde bulundurulmalıdır;

---

[1] Bitcoin 2008 yılında "Satoshi Nakamoto" tarafından deneysel olarak başlatılan, herhangi bir merkez bankası, resmi kuruluş vb. ile ilişkisi olmayan ve 3'üncü bir aracı kuruma ihtiyaç duymadan transferi yapılabilen bir tür dijital para birimidir. Küresel piyasalarda dolar ve avroya alternatif olarak lanse edilen Bitcoin'in kısaltması BTC'dir. Ulusal ve uluslararası para transferlerinde pratik ve hızlı olma gibi avantajlarının yanında, bu transferlerde gönderenin ve alıcının kimliğinin gizli tutulabilmesine imkan sağladığı için, yasa dışı ve usulsüz para transferlerinde sıklıkla tercih edilmektedir. Bitcoin'in güvenliği, aynı paranın birden fazla harcanamaması ve kimlik doğrulama gibi hususlar çoğunlukla şifreleme algoritmaları kullanılarak sağlanır. Ülkemizde Bitcoin konusundaki yasal boşluk nedeniyle, kullanımında sakınca olmadığına ilişkin görüşler bulunsa da, BDDK'nın 2013/32 sayılı basın açıklamasında, Bitcoin'in kanunen elektronik para olarak değerlendirilmediği, yapılan işlemlerde tarafların kimliklerinin bilinmemesi nedeniyle yasadışı faaliyetlerde sıklıkla kullanılabildiği, sonuç olarak mağduriyetlerin yaşanmaması adına vatandaşların Bitcoin'in muhtemel risklerine karşı dikkatli olması gerektiği ifade edilmiştir.

[2] Virüsün verdiği zararlara ilişkin detaylı rapor için Bkz. http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware

(1) Zararlı e-posta eklentisindeki dosya genellikle “E-Fatura.pdf.exe” veya “E-Fatura.pdf.scr” örneklerinde olduğu gibi “.exe”,“.scr” gibi çalıştırılabilir (executable) bir uzantıya sahiptir. Oysa, dokümanlar genellikle MS Office (*.doc, *.xls, *.ppt vb.), Adobe PDF (*.pdf) ve metin dosyaları (*.txt) uzantıları ile bitmektedir. İndirilen eklentideki dosyanın uzantısına dikkat edildiğinde kolaylıkla durum fark edilebilir. (Ancak, Windows’ta dosya uzantıları normalde gizli durumdadır ve görünür hale getirilmesi gerekmektedir).

(2) Hiçbir kurum, e-faturayı “.zip” dosyası içinde ve “*.exe” uzantılı dosya olarak göndermez. O nedenle bu tarz e-postalara şüphe ile yaklaşılmalı ve genel bir prensip olarak, e-posta ile gelen hiçbir “*.exe” vb. uzantılı çalıştırılabilir dosyaya tıklanmamalıdır.

b. Virüsün, ödeme için yönlendirdiği adreslerle irtibata geçilmemeli ve para gönderilmemelidir. Parayı almalarına rağmen şifreyi göndermeyen birçok durum olduğu bilinmektedir.

c. Virüs tarafından şifrelenen dosyaları editör yazılımları ile açıp içeriğini değiştirmek vb. işlemler, dosyaların kalıcı olarak bozulmasına sebep olmakta olup, daha sonra bir şekilde şifresi elde edilse bile dosyayı orijinal haline getirmek yani açabilmek mümkün olamayacağından, kesinlikle yapılmamalıdır.

ç. Virüsün tüm dosyaları şifrelemesi zaman alacağından, bilgisayarda “*.sifreli” veya “*.encrypted” uzantılı dosyalar görülmesi gibi işaretlerden virüsün çalıştığı ve şifrelemeye başladığı farkedilirse, en akılcı yöntem acilen bilgisayarın kapatılması ve takılı USB vb. tüm belleklerin çıkarılmasıdır. Kapatma işlemini standart usulle yani Windows’ta “Bilgisayarı Kapat”a basarak yapmak yerine, direkt olarak bilgisayarın güç düğmesine birkaç saniye basılı tutarak yapmak tercih edilmelidir. Unutulmamalıdır ki, her geçen saniyede onlarca dosya şifrelenmektedir. Bilgisayar kapatıldıktan sonra, henüz şifrelenmemiş dosyalar başka bir ortama (USB bellek vb.) alınana kadar, bilgisayar tekrar normal şekilde açılmamalıdır. Dosyaların güvenli ortama taşınması için bilgisayar konusunda detaylı bilgi sahibi kişilerden teknik yardım alınmalıdır (Bu işlem için genellikle bilgisayarı, harici bir medyada (CD, USB bellek) yer alan işletim sistemi ile başlatmak ve sonrasında hard disk’te yer alan dosyaları harici bir belleğe kopyalamak yöntemi izlenir).

d. Virüsten kurtulma işlemi iki adımdan oluşmaktadır: Virüsün bulaştığı sistemin temizlenmesi ve virüsün şifrelediği dosyaların şifresiz hale geri getirilmesi.

e. Virüsün Temizlenmesi:

(1) Virüsün birçok çeşidi, şu anda çoğu güncel antivirüs yazılımı tarafından tespit edilip temizlenebilmektedir. Dolayısı ile öncelikle virüsün bulaştığı bilgisayar, virüs tespit edilip temizlenene kadar, farklı antivirüsler ile taratılmalıdır.

(2) Ancak, virüsün birçok türevi olduğu ve sürekli olarak şekil değiştirdiği göz önüne alındığında, tespit edilememe ihtimali de oldukça yüksektir. Dolayısı ile tam olarak temizlik için, bulaştığı bilgisayara format atılarak, tekrar işletim sistemi kurulması gerekmektedir.

f. Virüsün Şifrelediği Dosyaların Şifresiz Hale Geri Getirilmesi:

(1) Üst maddede açıklandığı gibi virüsü temizlemek, virüsün şifrelediği dosyaların şifresini çözmemekte, sadece virüsün daha fazla dosyanızı şifrelemesini engellemektedir.

(2) CryptoLocker virüsü, şifrelemede RSA-4096 / AES-256 benzeri çok güçlü şifreleme algoritmaları kullanmaktadır. Dünyada şifre kırma yöntemlerinde gelinen son durumda, belirtilen algoritmanın kaba kuvvet (brute force) yöntemiyle kırılabilmesi için

katrilyonlarca yıldan çok daha fazla süre gerektiğinden, söz konusu algoritmalar kırılamaz kabul edilmektedir.

(3) CryptoLocker virüsünün birçok türevi olması, ayrıca saldırganların her bir bilgisayar için farklı anahtarlara sahip virüsler üretmesi nedeniyle, virüsün şifrelediği dosyaların çözülmesi için bir çözücü yazılım üretilmesi de mümkün olamamaktadır. Dolayısı ile **şifrenin çözülmesi günümüz şartlarında şifre anahtarını bilmeden mümkün değildir** (CryptoLocker virüsüne karşı çözüm geliştirdiğini ifade eden internetteki birçok hilekâra karşı dikkatli olunmalıdır).

(4) Halihazırda genel şifre çözme amaçlı geliştirilen yazılımlar, maalesef CryptoLocker için kullanılamamaktadır çünkü CryptoLocker'ın 20'den fazla bilinen türevi vardır ve sürekli değişiklik arz edebilmektedir.

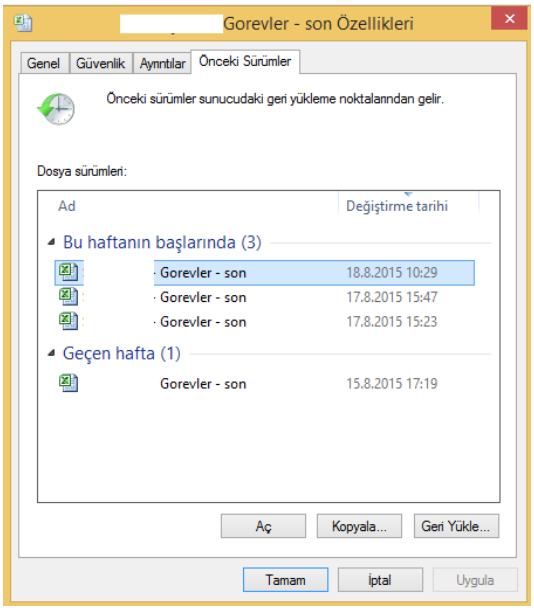
(5) Denenmesi gereken ilk işlem, virüsün dosyaları şifrelemeyi müteakip orijinal halini hızlı silmiş olabileceği umularak, virüsün bulaştığı sürücülerde veri kurtarma (File recovery) yazılımları ile silinmiş olan orijinal dosyaları geri getirmeye çalışmaktır. Geri getirme ortamı olarak harici USB disk/bellekler tercih edilmelidir.

(6) Yapılabilecek diğer işlem ise, dosyaların virüs tarafından şifrelenmeden önce alınmış bir yedeği varsa, o yedeğin kullanılmasıdır. Bu kapsamda, genel tedbirler olarak;

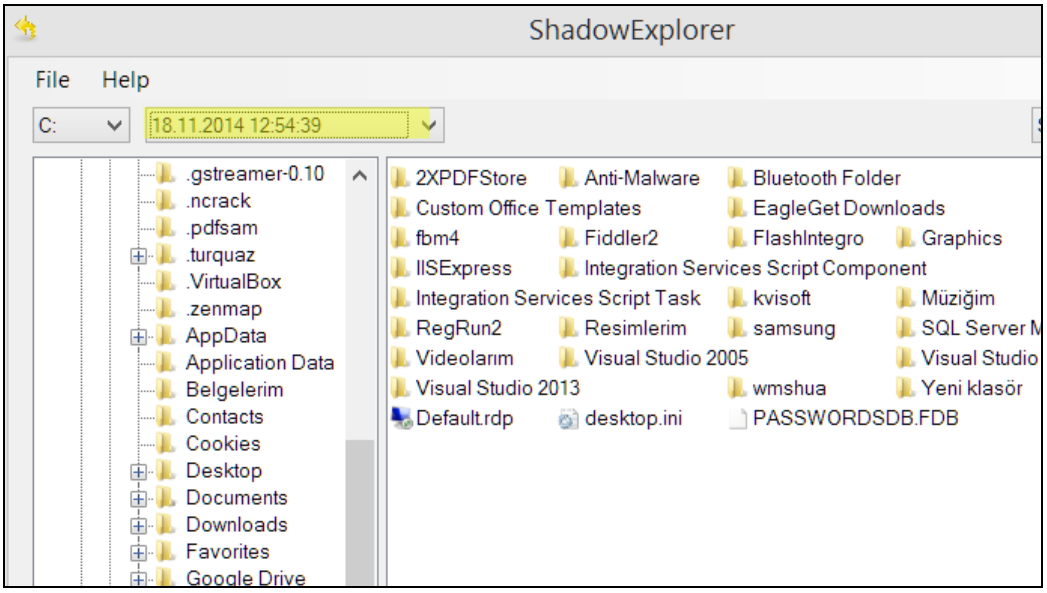
(a) Kritik dosyalarınızın belirli aralıklarla yedeğini tek yazımlık CD/DVD'lere almanız tavsiye edilmektedir (Tek yazımlık DVD'lerde bulunan dosyaların, DVD'nin yapısından dolayı virüsler tarafından şifrelenmesi teknik olarak mümkün değildir).

(b) Bilgisayarlardaki işletim sistemlerinde, dosyaların değişmesi (silinmesi, içeriğinin değişmesi vb.) durumunda otomatik olarak bir önceki versiyonunun arşivlenmesini sağlayan imkânlar bulunmaktadır. Bu kapsamda; Windows XP Service Pack 2 ve üstü, Windows Vista ve Windows 7 işletim sisteminde "Shadow Copy", Windows 8 işletim sisteminde ise "File History" işlevleri aktif hale getirilebilir. Bu işlevler açık olan bilgisayara CryptoLocker bulaşsa bile, şifrelenmeden önceki versiyonlara geri dönülmek suretiyle virüsün zararının telafi edilmesi sağlanabilir. Ancak; CryptoLocker'ın bazı gelişmiş versiyonlarında, oturumu açan kullanıcının yetkisi var ise, virüs, işletim sisteminin tuttuğu eski dosya versiyonlarını da silmektedir. Bu durumda bu işlevler maalesef işe yaramayacaktır. **Bu nedenle, günlük kullanımda sınırlı (standart) yetkide kullanıcı ile oturum açılması ve sadece yönetici yetkisi gerektiren durumlarda (yeni yazılım kurmak vb.) yönetici (administrator) yetkisindeki kullanıcıların kullanılması, virüsün zararını en aza indirecektir.**

(c) Bir dosyanın versiyonlarını görmek için, dosyayı seçip sağ tıkladığınızda aşağıda örneği görülen, "Önceki Sürümler" sekmesine bakılabilir. Bu sekmeyi boş görüyorsanız, bilgisayarınızda "Shadow Copy" işlevi pasif veya o dosyanın versiyonu oluşmamış demektir.



(ç) Virüsün şifrelediği klasörlerdeki dosyaları, dosyaların versiyonlarından tek tek geri almak uzun zaman alabilir. Bu nedenle, "Shadow Copy" ile tutulan dosya versiyonlarını tarih bazlı görebilmek ve toplu olarak geri yüklemek için, internetten "ShadowExplorer" isimli ücretsiz yazılım indirilmesi tavsiye edilir. ShadowExplorer yazılımının ana ekranı aşağıdaki gibi olup, virüsün bulaşma tarihinden önce bir geri yükleme noktası seçerek, dosyalara sağ tık ve "Export" ile güvenli bir ortama şifresiz hallerini almasını sağlayabilirsiniz. Eğer, seçtiğiniz sürücü ("C:" gibi) karşısında kayıt göremiyorsanız gölge kopyanız yok veya virüs tarafından silinmiş demektir. Bu durumda yapabileceğiniz bir işlem maalesef kalmamaktadır.



(d) "Export" ile aldığınız şifresiz dosyaları, bilgisayarın virüs temizliğini müteakip bilgisayarınıza geri kopyalamanız önerilir.

(e) "Shadow Copy", "File History" ve "ShadowExplorer" hakkında detaylı bilgi ve yapılandırma açıklamaları için, 4.maddede yer alan "Faydalı Bağlantılar" bölümüne bakabilirsiniz.

g. BİLGİ SİSTEM İŞLETMENLERİNCE ALINABİLECEK TEDBİRLER:

(1) Güncel tutulan bir antivirüs yazılımı kullanmak virüsün tespitinde son derece önemlidir ancak şu hususlar bilinmelidir;

(a) Virüs kullanılarak alınan fidyelerden ciddi gelir elde edilebilmesi nedeniyle virüsün birçok çeşidi (hatta son dönemlerde mobil cihazlarda çalışan türleri de görülmeye başlanmıştır) ortaya çıkmış olup, halen 20'den fazla CryptoLocker türevi tespit edilmiştir. Bu çeşitlilik, virüse karşı etkin bir tedbir geliştirilmesini oldukça zorlaştırmaktadır.

(b) Antivirüs firmaları, ortaya çıkan türlere ilişkin virüs imza veri tabanlarını güncellese bile, virüsün kodunda ufak bir değişikliğin yapılması durumunda, antivirüs yazılımları virüsü tespit edememektedir.

(c) Antivirüs yazılımlarında ileri düzeyde bir tespit metodu olan Davranışsal (heuristic) Tespit Yöntemi, maalesef virüsün tespitinde kullanılamamaktadır. Çünkü virüsün yaptığı yeni dosya oluşturma ve silme işlemi, çoklu dosya taşıma esnasında da gerçekleştiğinden, bu işlemin antivirüs tarafından şüpheli kabul edilerek engellenmesi durumunda, normal dosya işlemlerinde de sorunlarla karşılaşılmaktadır.

(2) İşletim sistemi, kurulu program ve eklentilerin güncellemeleri aksatılmadan yapılmalıdır.

(3) Dosya sunucuları yedeklerinin daha sık alınması sağlanmalıdır.

(4) Dosya sunucularında, versiyonlamayı sağlayan "Shadow Copy" işlevi aktif olmalıdır.

(5) Kritik dosyaları barındıran dosya sunucusu olmayan sistemlerdeki bilgisayarlarda, verilerin belirli aralıklarla tek yazımlık CD/DVD'lere yedeklenmesi gerektiği unutulmamalıdır.

(6) %AppData% klasöründen bir yazılım çalışmasını engelleyecek politika üretilebilir. Bu grup politikası olarak da uygulanabilir. Bu konuda detaylı bilgi ve açıklamaları "Faydalı Bağlantılar" maddesindeki linklerde bulabilirsiniz.

3. SONUÇ:

a. Cryptolocker virüsünün ülkemizde genellikle sahte e-faturalarla yayıldığı biliniyor olsa da, saldırganların her zaman virüsü yayacak yeni yöntemler bulabilecekleri unutulmamalıdır.

b. Virüse karşı genel bir siber güvenlik tedbiri olarak, internetten gelen dosyalara şüpheci yaklaşılmalı, dosyanın kaynağı ile türünden tam olarak emin olmadan dosyalar açılmamalıdır.

c. Sonuç olarak; siber güvenlik konularındaki genel bilgi eksikliği nedeniyle, bilgisayarlara kolaylıkla virüs bulaşmaktadır. Oysa siber güvenliğe ilişkin temel güvenlik tedbirlerini uygulayarak birçok saldırıdan korunmak mümkündür. Bu noktada, vatandaşlarda siber farkındalığın artırılması ve kurumların siber güvenlik personelinin uzmanlık derecesinin üst seviyede tutulmasına yönelik çalışmaların yapılması oldukça önem arz etmektedir.

4. FAYDALI BAĞLANTILAR:

a. “Shadow copy” açıklamaları:

http://www.howtogeek.com/56891/use-windows-7s-previous-versions-to-go-back-in-time-and-save-your-files/

b. “File history” açıklamaları:

http://blogs.msdn.com/b/b8/archive/2012/07/10/protecting-user-files-with-file-history.aspx

c. “ShadowExplorer” yazılımı:

http://www.shadowexplorer.com

ç. “%APPDATA%” klasöründen bir dosyanın (exe vb.) çalıştırılamaması için politika oluşturmak:

http://support.microsoft.com/kb/310791

http://technet.microsoft.com/en-us/library/cc786941(v=ws.10).aspx