İleri Teknoloji Bilimleri Dergisi
Journal of Advanced Technology Sciences
ISSN:2147-3455

CRYPTOLOCKER SALDIRILARININ İNCELENMESİ

Mustafa ERİŞ[1] Mustafa KAYA[2]

[12] Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği Bölümü, 23119, Elazığ, TÜRKİYE
meris@firat.edu.tr

Özet- Günümüzde internetin yaygın bir şekilde kullanılması ile beraber, bilgi güvenliğini tehdit eden virüsler, zararlı yazılımlar, casus yazılımlar, truva atları gibi unsurlar da gün geçtikçe çoğalmaktadır. Bireyler, kamu kurumları ve özel kuruluşlar bu tür tehditler tarafından zarar görebilmektedirler. Bu tehditlerden korunmak için bilgi güvenliği konusunda ciddi tedbirlerin alınması gerekmektedir. Son zamanlarda sistemleri ve kullanıcıları en hızlı etkileyen elektronik veri güvenliği tehditlerinden biri de fidye yazılımı (Ransomware) türünde olan Cryptolocker virüs yazılımlarıdır. Cryptolocker girdiği sistemdeki dosyaları sahibinin istemi dışında şifreleyerek, ulaşılmasını engelleyen bir yazılımdır. Bu yazılım kişisel veya kurumsal bilgileri kendi bulunduğu ortamda şifreleyerek sahibinin erişimini imkansız hale getirmektedir. Bu virüsün etkisi altında kalan kişi veya kurumlar önemli verilerinin kaybedilmesi ile veya virüs yazılımcısının istediği maddi miktarları ödemekle yüz yüze kalmaktadırlar. Bu çalışmada Cryptolocker zararlı yazılımı incelenerek; yazılımın kullandığı şifreleme algoritmaları, etkilediği sistem öğeleri ve alınabilecek önlemler ortaya konmuştur.

Anahtar Kelimeler- Cryptolocker, Zararlı Yazılım, Bilgi Güvenliği, Fidye Yazılımları

ANALYSIS OF CRYPTOLOCKER ATTACKS

Abstract- Nowadays in parallel to the widespread use of the internet, elements such as viruses, malwares, spywares and trojan horses which threaten information security are increasing. Individuals, state agencies and private institutions can be damaged massively by this kind of threats. Serious precautions about information security must be taken to prevent this kind of threats. Cryptolocker, which is a ransomware type virus, is one of the electronic data security threats which are affecting systems and users rapidly. Cryptolocker is a software that blocks access of the users to their files by encrypting. Users whose data under the control of this malware have no choice but losing their data or paying the ransom this malware demands. In this study, Cryptolocker malware is analyzed and encryption algorithms used by the malware, system elements that affected by the malwares and precautions to be taken are demonstrated.

Key Words- Cryptolocker, Malware, Information Security, Ransomwares

1. GİRİŞ (INTRODUCTION)

Son yıllarda bilgi teknolojilerinin gelişmesi ve yaygınlaşmasıyla birlikte kullanıcıları olumsuz yönde etkileyen yazılım ve virüslerin sayısında da artış görülmektedir. Bu zararlı yazılımlar içerisinde en etkili olanlarından birisi de 2005 yılında ortaya çıkmış olan ransomware yazılımlardır [1]. Bu yazılımlar reklamlar, bilgilendirme mailleri ve sosyal mühendislik saldırıları gibi yöntemlerle kullanıcıların bilgisayarlarına bulaşabilmektedir[2]. Cryptolocker da ilk olarak 2013 yılında ortaya çıkan ve Windows işletim sistemi kullanan bilgisayarları hedef alan bir ransomware yazılımıdır [3]. Bu zararlı yazılım bulaştığı sistemlerdeki kritik dosyaları çözülmesi çok zor olan şifreleme algoritmaları ile şifrelemektedir. Saldırganlar tarafından şifrelenen her sistemin anahtarı bir sunucuda tutulur ve kullanıcı saldırganın istemiş olduğu ücreti ödemediği durumda veri dosyalarını kaybetmesi ile tehdit edilir. Mağdur talep edilen ücreti sınırlı bir süre içinde ödemesi için Bitcoin, MoneyPack, Ucash ve Kashu gibi sanal para sistemlerine yönlendirilmektedir[3]. Genellikle veriyi kurtarma girişimlerini engellemek için belirli bir ödeme süresi verilir ve bu süre sahibin veriyi kurtarmak için denediği hatalı şifre girişlerinde azaltılmaktadır.

Cryptolocker dünya çapında birçok bilgi kaybı ve maddi zarara yol açmıştır. Ortaya çıkmasının ikinci ayında yaklaşık 30,000 sistemi etkilemiştir ve üç ayda yaklaşık 30 milyon dolar para kaybına yol açmıştır. Etkisinin büyük olması cryptolocker kopyalarının oluşturulmasını da tetiklemiştir ve birçok benzer yazılım ortaya çıkmıştır[4].

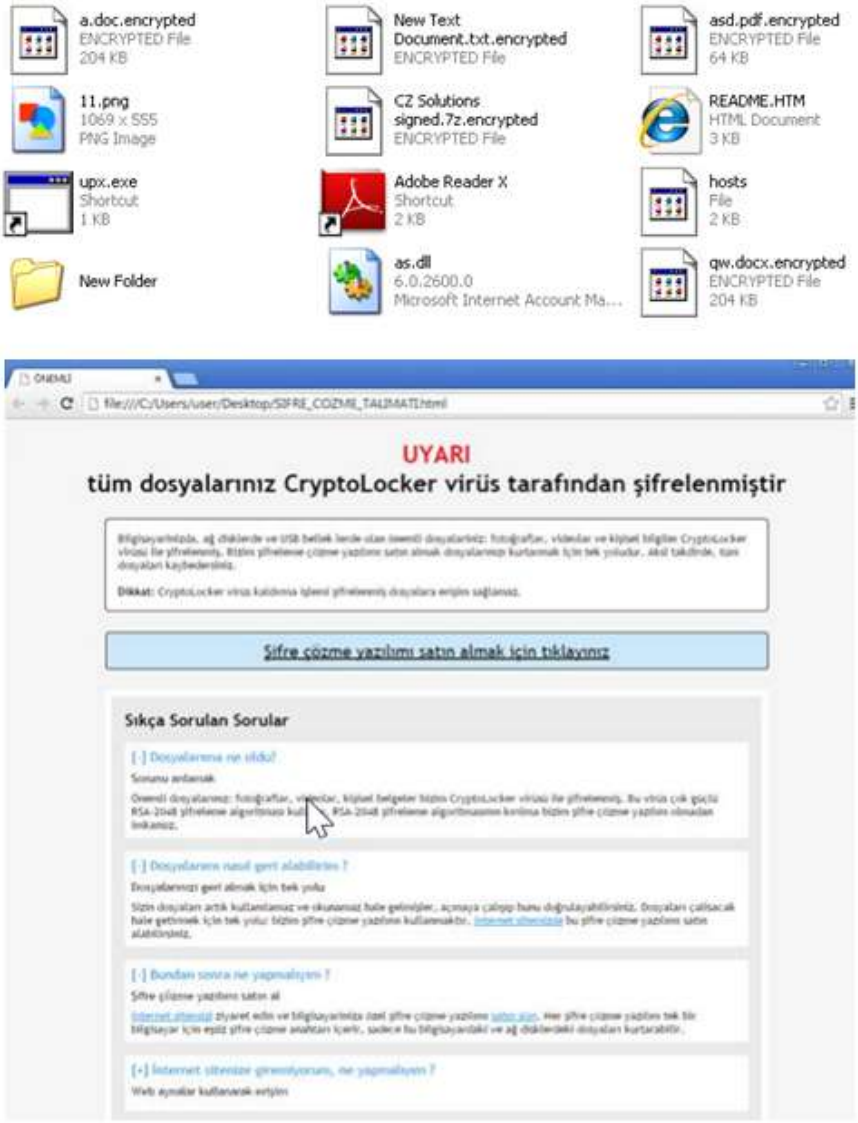
Kişilere ve kurumlara büyük zarar verebilen bu zararlı yazılımlara karşı yeterli önlemlerin alınması gerekmektedir. Bu nedenle çalışma prensibi ve korunma yöntemlerinin öğrenilmesi önemlidir. Bu çalışmada bu tür yazılımlardan zarar görmemek için yapılması gerekenler ve bu saldırıların çalışma prensibi ortaya koyulmuştur.

1. CRYPTOLOCKER ZARARLI YAZILIMI (CRYPTOLOCKER MALWARE)

2.1. Bulaşma ve Dağıtım Şekli (Infection and Distribution Method)

Cryptolocker'lar güvenilir gibi algılanan kurumlardan gelen virüslü e-mail ekleriyle yayılmaktadır. Ülkemizde ilk olarak internet faturası görünümündeki maillerle ortaya çıkmıştır.

Resim 1. TTNet Fatura Bilgisi Görünümlü Cryptolocker Virüsü (TTNET billing loking Cryptolocker Virüsü)



Resim 2. Dosyaların Şifrelendikten Sonraki Hali ve Çıkan Uyarı Ekranı (Notification Screen After Files are Encrypted)

Gelen mail eklerine sıkıştırılmış veya çalıştırılabilir dosyalar eklenmektedir. Kullanıcı pdf görünümlü bir dosya görmektedir. Aslında bu dosya .exe uzantılı bir Cryptolocker dosyasıdır. Dosyanın .exe uzantılı olduğunun anlaşılamaması için Windows'un varsayılan olarak aktif olan dosyaların uzantılarını gizleme özelliğinden yararlanılır. Kullanıcı dosyayı açmak istediğinde zararlı yazılım, sistemi ele geçirmiş olur.

Cryptolocker'ı yaymak için kullanılan mailler rastgele üretilen domainlerden kullanıcılara gönderilmektedir. Bu rastgele domainler Domain Generation Algorithm (DGA) denilen bir yöntemle üretilmektedir. Günde 1000 domain oluşturabilen bu yöntem virüs analistleri ve güvenlik uzmanlarının, enfekte bilgisayarların bağlantı kurduğu yönetim sunucularını bulup etkisiz hale getirmelerini zorlaştırmak için kullanılmıştır. Ayrıca bu yöntem sayesinde virüslerin gönderildiği domainler engellense bile yerine oluşturulacak domainler bilinmediğinden, diğer bilgisayarlar yeni gelecek mail ve dosyalara açık olurlar. DGA ile oluşturulan domainler 12 ile 15 arasında rastgele karakter ve 7 olası üst seviye alan adından oluşur. Cryptolocker tarafından oluşturulan bazı domainler Tablo 1'de gösterilmiştir.

Tablo 1. DGA ile Üretilen Bazı Domainler (Some Domains Created by DGA)

Domain Adı	Çıkış Tarihi
qwlpubwopsyj.org	C2 domain, September 9, 2013
sypdwysctilgr.net	C2 domain, September 9, 2013
txeuntcemcwj.biz	C2 domain, September 10, 2013
qqkoluhwexlr.biz	C2 domain, September 10, 2013
xeogrhxquuubt.com	C2 domain, September 10, 2013
qaaepodedahnslq.org	C2 domain, September 10, 2013
vbitnxdgsiwg.biz	C2 domain, September 11, 2013

2.2. Teknik Özellikler (Technical Specifications)

Cryptolocker yazılımlarında anahtar dağıtımı için RSA (Rivest – Shamir – Adleman) asimetrik şifreleme algoritması kullanılmaktadır. Algoritma sonucu elde edilen anahtar AES-256 (Advanced Encryption Standart) şifreleme anahtarını şifrelemek için kullanılır. Cryptolocker virüsü yerleştiği makinedeki dosyaları AES-256 ile şifrelemektedir[11]. RSA anahtar dağıtımı için 2048 bitlik anahtar boyutu kullanılmaktadır. RSA anahtar dağıtım algoritmasından üretilen özel anahtar cryptolocker'ın yayınlandığı sunucuda depo edilir. Şifreleme işleminin yanı sıra yerleştiği bilgisayarda kayıt defterine girilen kod ile cryptolocker'ın bilgisayar her açıldığında çalışması sağlanmaktadır. Kullanılan anahtar boyutları 128 bitten büyük olduğu için kaba kuvvet (brute-force) saldırısıyla kırılması imkansızdır. Bunun nedeni, şifrelenen verilerin kırılabilmesi için en kötü durum için 2^{256} işlem yapılması gerekmektedir. Günümüzde bu işlemi kabul edilebilir bir zamanda yapabilecek bilgisayar sistemleri bulunmamaktadır. Cryptolocker kullanıcıların önemli verilerinin tutulduğu jpg, doc, docx, xls, xlsx, cad, pdf vb. uzantıya sahip olan dosyaları şifreleyebilmektedir. Bu nedenle sistemin bu tip saldırıları maruz kalmaması için çeşitli önlemler alınması gerekmektedir.

2.3. Şifreleme Algoritmaları (Encryption Algorithms)

Cryptolocker şifreleme işlemleri için çok güçlü şifreleme algoritmaları olan AES-256 ve RSA-2048 algoritmalarını kullanır. RSA-2048 anahtar dağıtımı için kullanılır. AES-256 ise block chipper şifreleme için kullanılma ktadır. RSA ve AES in özellikleri aşağıda verilmiştir.

2.3.1 RSA Şifreleme Algoritması (RSA Encryption Algorithm)

Çok büyük tam sayıların çarpanlara ayrılmasının algoritmik zorluğundan yararlanarak tasarlanan RSA en bilinen açık anahtarlı şifreleme algoritmasıdır[9]. Birçok uygulama alanı olmasına rağmen RSA genelde aşağıdaki iki amaç için kullanılır.

- Özellikle anahtar iletimi için küçük data parçalarını şifreleme
- İnternette dijital sertifikalar için dijital imzalar

Cryptolocker da anahtar oluşturmak ve dağıtmak için RSA-2048 algoritmasından yararlanmıştır.

2.2.1.1. RSA Anahtar Üretim Adımları

- Büyük bir sayı oluşturmak için birbirinden farklı iki asal sayı seçilir. Bu sayılara p ve q denir.
- İki asal sayının çarpımını asal çarpanlarına ayırmak diğer sayılardan daha zor olduğundan N büyük sayısı p ve q sayılarının çarpımı olarak hesaplanır.
  $N = p.q$ (1)
- N sayısının kendisinden küçük ve kendisiyle aralarında asal olan sayı adedi bulunur buna totient fonksiyonu denir ve φ(N) şeklinde gösterilir.
- N sayısının totient değeriyle aralarında asal ve bu değer ile 1 arasında bir e sayısı belirlenir.
- $1<e<\varphi(N)$, EBOB(e,φ(N))=1
- Denklem (2)'de verilen ifadeyi sağlayacak şekilde bir d sayısı hesaplanır. Bulunan d sayısı gizli anahtarı hesaplamada kullanılır.
  $d \times e = (mod\ \varphi(N))$ (2)

Burada p,q ve φ(N) değerleri, d değerinin bulunmasında kullanıldığı için gizlidir. Elde edilen (N,e) çifti açık anahtarı, (N,d) çifti ise gizli anahtarı oluşturur. Açık anahtar AES-256 algoritmasına giriş olarak verilirken gizli anahtar da cryptolocker'ın kontrol ve komuta sunucularında depo edilir.

2.3.2 AES Şifreleme Algoritması (AES Encryption Algorithm)

AES şifreleme algoritması, John Daemen ve Vincent Rijmen tarafından Rjindael ismiyle geliştirilmiştir[10]. AES şifreleme, verilerin alt bytelara ayrılması (SubBytes), satırları kaydırılması (ShiftRows), sütunları karıştırılması (MixColumn) ve anahtar eklenmesi (AddKey) adımlarıyla yapılır[11]. Bu algoritma ile veri blokları şifreleme adımları tekrarlanarak şifrelenir. Bu adımlar her tekrarda gerçekleştirilmektedir. AES algoritması şifrelenecek verileri 128 bitlik bloklar halinde ve 128,192 ve 256 bitlik anahtar ile şifreler. Anahtar uzunluklarına göre çevrim sayıları Tablo 2'de verilmiştir [9].

Tablo 2. AES Anahtar Uzunlukları ve Çevrim Sayıları (Key Lengths and loop counts of AES algorithm)

Anahtar Uzunluğu	Çevrim Sayısı
128	10
192	12
256	14

Şifreleme işlemine başlamadan önce şifrelenecek veri 128 bitlik parçalara bölünür ve durum matrisi denilen 4X4 boyutundaki bir matrise yerleştirilir bundan sonra yapılacak işlemler bu matris üzerinde yapılır. Durum matrisi oluşturulduktan sonra ilk olarak bayt değiştirme işlemi gerçekleştirilir. Bu adımda durum matrisine eklenen her bir eleman daha önceden standart olarak belirlenmiş S-Box'daki değerler ile değiştirilir. Satır kaydırma işleminde durum matrisindeki satırlar 1 satır sabit kalmak şartı ile kaydırılır. 2. , 3. ve 4. satırlar sırasıyla 1,2,3 byte sola kaydırılır. Daha sonra sütun karıştırma işlemi gerçekleştirilir. Bu işlem sırasında durum matrisindeki her sütun sabit bir matris ile çarpılır ve karışması sağlanır. Son adım olan anahtar ekleme işleminde ise anahtar byte larına ayrılır ve sırayla durum matrisi elemanları ile XOR işlemine tabi tutulur. Böylece işlemler sonuncunda veri şifrelenmiş hale dönüşür.

2.4. Zararlı Yazılımın Kullandığı Sistem Öğeleri (System Components That Malware Use)

Cryptolocker yazılımı Windows işletim sistemlerinde sistem versiyonuna göre farklı dosya dizini ve kayıt defteri anahtarlarını kullanmaktadır[10]. Yürütülebilir yazılım dosyalarını dizinlerde çalıştırırken şifrelenmiş dosyaları saklama için de bir kayıt defteri anahtarı oluşturur. Daha sonra oluşturulan bu dosyalardan şifreleme ve çalıştırma işlemleri yönetilir. Cryptolocker'ın oluşturduğu dosyalar ve dosya yolları;
%AppData%\"rastgele_isim.exe" veya %AppData%\{<8 karakter>-<4 karakter>-<4 karakter>-<4 karakter>-<12 karakter>}.exe formatında olabilmektedir[11].
Ayrıca Cryptolocker farklı işletim sistemlerinde farklı dosya yollarını kullanır. Cryptolocker'ın kullandığı dosya yolları Tablo 3'de verilmiştir.

Tablo 3. Cryptolocker'ın Kullandığı Dosya Yolları (File Paths Used By Cryptolocker)

Windows xp	Windows Vista\7\8
C: \ Documents and Settings \ <User> \ Application Data \	C: \ Users \ <User> \ AppData \ Local \
C: \ Documents and Settings \ <User> \ Local \ Application Data \	C: \ Users \ <User> \ AppData \ Local \

Cryptolocker kendisini baştan çalıştırmak, sistem hakkındaki bilgileri ve şifreleme anahtarını saklamak ve sisteme bulaştığı zamanı kaydetmek için kayıt defteri anahtarları oluşturur. Bu anahtarlar Tablo 4'de verilmiştir.

Tablo 4. Cryptolocker'ın Oluşturduğu Kayıt Defteri Anahtarları (Registry Keys Created by Cryptolocker)

KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker_<version_number>"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker_<version_number>"

Cryptolocker'in güncel versiyonu Cryptolocker 0388 in kayıt anahtarındaki * ifadesi zararlının güvenli modda dahi çalıştırılmasını sağlamaktadır. Ayrıca konfigürasyon bilgisi ve şifrelenmiş dosyaların kaydını tutmak için de bir anahtar oluşturulur. Önceki versiyonlarda HKEY_CURRENT_USER\Software\CryptoLocker anahtarı kullanılmıştır. Geçerli versiyonda ise konfigürasyon bilgisini kaydetmek için HKEY_CURRENT_USER\Software\CryptoLocker_0388 anahtarı kullanılmaktadır.[11] Bu anahtar PublicKey, VersionInfo ve Wallpaper olmak üzere 3 değer içerir. PublicKey değeri

dosyaları şifrelemek için kullanılan açık anahtarı içerir. VersionInfo değeri zararlı yazılımın versiyonu, sunucusunun ip adresi ve yüklenme tarihi gibi bilgileri içerir. Wallpaper değeri ise enfekte bilgisayarın masaüstünde arka plan olarak gösterilen duvar kağıdı ile ilgili bilgileri içerir.

2.5. Korunma Yöntemleri (Prevention Methods)

Kullanıcı bilgisayarlarında alınabilecek önlemler ile Cryptolocker'dan etkilenmemek büyük oranda mümkündür. Sistem cryptolocker tarafından şifrelendikten sonra dosyaların geri dönüşünün çok zor olmasından dolayı bu tür virüslerden korunmak için öncelikle yararlı kullanım alışkanlıkları edinilmelidir. Bu kapsamda yapılması gerekenler aşağıdaki gibi sıralanabilir.

- Düzenli olarak önemli verilerin yedeği alınmalıdır. Ayrıca yedek alınan birimin internet ve bilgisayarla bağlantısı kesilmelidir veya bulut depolama kullanılmalıdır.
- Windows dosya uzantıları görünür hale getirilmelidir.
- Gelen mail ve mesajlardaki yürütülebilir dosya sadece gönderici güvenilir ve tanıdıksa çalıştırılmalıdır.
- Windows otomatik güncelleştirme özelliği aktif edilmeli, en son virüs ve zararlı yazılım veri tabanlarını tanıması sağlanmalıdır.
- Kaliteli antivirüs programları kullanılmalı ve güncel tutulmalıdır.
- E-posta servislerinde.exe uzantısı içeren maillere filtre uygulanabilir.
- Windows Grup ve Yerel İlke düzenleyiciler konfigüre edilebilir. Bu yöntemle Tablo 3'de gösterilen dosya yollarından herhangi bir yürütülebilir dosyanın çalışması engellenebilir.
- Aynı domainden mail gelme olasılığına karşı bilinen tüm cryptolocker yayan domainlerin, bulunulan ağ ile bağlantı kurması engellenebilir. Çünkü, cryptolocker kontrol ve yönetim sunucularından herhangi birisine başarılı bir şekilde bağlanamadan şifreleme işlemine başlamaz.

Bu gibi yöntemlerle cryptolocker zararlı yazılımından korunma seviyesi artırılabilmektedir. Bu önlemler dışında bilgisayar enfekte olduktan sonra da yapılacak işlemler ile büyük bir sistemin zarar görmesi engellenebilir veya virüsün etkisi azaltılabilir. Cryptolocker zararlı yazılımının çalıştırıldığının farkına vardıktan sonra da aşağıda sıralanmış önlemler alınarak büyük çaplı zarar görmekten kaçınılabilmektedir.

- Virüsün çalıştığı anlaşılır anlaşılmaz internetten ve bulunulan ağdan çıkılmalıdır. Böylelikle virüsün internet üzerinden tüm ağa yayılma riski engellenmiş olur.
- Değişen dosyaları diğer cihaz ve sunucularda da değiştiren senkronizasyon programları devre dışı bırakılmalıdır.
- Virüs, anti-virüs programları veya el ile silinmeli ve Bölüm 3.4.'de verilen kayıt defteri anahtarları temizlenmelidir.
- Shadow Copy gibi Windows'un otomatik olarak oluşturduğu geri yükleme yöntemlerinden yararlanılabilir.

Bu yazılıma karşı önlem alabilmek için Shadow Copy gibi otomatik geri yükleme noktaları oluşturan ve yedek alan yazılımların kullanılması önerilmiştir. Ancak Ekim 2014'te Hollanda' da ortaya çıkan Cryptolocker'ın yeni sürümü Shadow Copy gibi programları devre dışı bırakmaktadır[11].

Şekilden sonra bir satır boşluk bırakarak metne devam ediniz.

3. SONUÇ VE TARTIŞMA (CONCULUSION AND DISCUSSION)

Bu çalışmada günümüzde kullanıcıların sık karşılaştığı Cryptolocker zararlı yazılımlarının çalışma prensipleri ve alınabilecek önlemler ortaya konmuştur. Bilgisayar kullanıcıları günlük aktivitelerini gerçekleştirirken farkında olmadan bu türde saldırılara maruz kalmakta ve önemli

bilgi ve para kayıpları yaşamaktadır. Sistemdeki verilerin kullanıcı açısından önemi neticesinde bu saldırganlara maddi ödeme yapma zorunluluğunu ortaya çıkmaktadır. Bu nedenle kullanıcıların alabileceği önlemler ile bu saldırılardan büyük ölçüde korunması mümkün olmaktadır. Ayrıca yazılımın sisteme enfekte olmasından sonraki süreçlerde doğru adımlar izlenerek zararın etkileri azaltılabilmektedir. Bu nedenle kullanıcıların güvenliğinin sağlanabilmesi için farkındalık yaratılması büyük önem taşımaktadır. Bu çalışma ile yazılımın teknik çalışma prensipleri, etki alanları incelenip, yazılıma karşı alınabilecek önlemler açıklanarak, kullanıcıların zarar görmesi engellenmiş olacaktır.

5. KAYNAKLAR (REFERENCES)

[1]. Gazet, A., (2008), Comparative analysis of various ransomware virii, Journal of Computer Virology and Hacking Techniques, 77-90

[2]. Luo, X. , MSIS & Liao, Q., (2007), Awareness Education as the Key to Ransomware Prevention, Information Systems Security, 195-202

[3]. Cryptolocker Malware Analiz Raporu (2014), UITSEC, http://uitsec.com/publics/docs/cryptolocker-dokuman.pdf

[4]. S. Mansfield-Devine, (2014), The dark side of advertising, Computer Fraud & Security, 5-8

[5]. Kotov V., Rajpal M., (2014), Understanding Crypto-Ransomware, http://www.bromium.com/sites/default/files/bromium-report-ransomware.pdf

[6]. Christof Paar, Jan Pelzl, (2010), Understanding Cryptography, 173-179

[7]. Daemen, J., Rijmen, V., (2002),The Design of Rijndael: AES - The Advanced Encryption Standard

[8]. Certeza, R.A., (2013), Trend Micro, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3132/ransomware-raises-the-stakes-with-cryptolocker, Son erişim Tarihi: 20.05.2015

[9].İnternet: http://cryptographicprocessor.weebly.com/uploads/2/4/5/3/24530999/aes.pdf (Son Erişim Tarihi, 4.07.2015)

[10]. İnternet:https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24786/en_US/McAfee_Labs_Threat_Advisory_Ransom_Cryptolocker.pdf (Son Erişim Tarihi, 14.06.2015)

[11]. İnternet: http://resources.infosecinstitute.com/cryptolocker/ (Son Erişim Tarihi, 15.07.2015)