TESLACRYPT FİDYE YAZILIM VİRÜSÜNÜN TESPİTİ, TEKNİK ANALİZİ VE ÇÖZÜMÜ

***

DETECTION, TECHNICAL ANALYSIS AND SOLUTION OF TESLACRYPT RANSOMWARE VIRUS

İlker KARA[*]

Öz

Bilişim teknolojilerinde yaşanan hızlı gelişmeler internet kullanıcılarının hayatında pek çok şeyi kolaylaştırmışken, kötü niyetli kişilerinde amaçlarına daha hızlı ulaşması için yeni olanaklar sağlamaktadır. İlk tasarım amacından tamamen uzaklaşan zararlı yazılımlar, günümüzde profesyonel suçlular tarafından siber terörizmden fidye istemeye kadar geniş bir uygulama alanı için tasarlanmaktadır. Bu suçlular çok çeşitli yöntemler ve taktikler geliştirerek amaçlarına kolaylıkla ulaşmakta, bu duruma maruz kalma olasılığı kullanıcıların korkulu rüyası haline gelmektedir. Son günlerde dünya genelinde TeslaCrypt olarak adlandırılan yeni nesil fidye yazılım siber saldırı vakaları görülmeye başlamıştır. TeslaCrypt, kullanıcılara e-mail yoluyla ulaşarak ekinde bulunan zararlı yazılımın çalıştırılması ile sistemdeki birçok dosyayı şifrelemektedir. Kullanıcının şifrelenmiş dosyalara erişim sağlayabilmesi için fidye göndermesini istemektedir. TeslaCrypt'nin sebep olduğu bu durum için çalışmalar devam etmekle birlikte hala kesin çözüm bulunamamıştır. Bu çalışma, TeslaCrypt tehditinin tespiti, hedef sisteme sızma, sistemdeki dosya-dizin hareketlerinin teknik analizini ve çözümünü içermektedir. İncelemeler; hem statik hem de dinamik yöntemlerle gerçekleştirilmiştir. Çalışma sonucunda fidye yazılımının neden olduğu şifrelerin kırılabilir olduğu gösterilmiştir.

Anahtar Kelimeler: *Zararlı Yazılım Analizi, Fidye Yazılımı, Kriptokitleyici.*

Abstract

Although the rapid developments in information technologies have facilitated numerous things in the lives of Internet users, these developments also allow malicious people to reach their goals faster. Malicious software that completely drift away from their initial design goal are now being designed by professional criminals for a wide range of applications from cyber terrorism to ransom demands. These criminals reach their goals easily by developing a variety of methods and tactics, and the possibility of being exposed to this situation becomes the worst nightmare for the users. Recently, a new generation of Ransomware, known as TeslaCrypt, has begun to be seen worldwide. TeslaCrypt reaches users through e-mail and encrypts many files in the system after execution of its payload found in the e-mail attachment. It demands ransom to allow access to encrypted files of the user. Although there are continuing works to find a solution to this problem caused by TeslaCrypt, there is still no definitive solution. This study discusses the detection of TeslaCrypt threat, and technical analysis on its infiltration into the target system and file-directory actions in the system and solution. The analysis has been performed by both static and dynamic methods. As a result of the study, it was shown that the passwords caused by the ransomware virus broke the password.

Keyword: *Malware analysis, Ransomware, Cryptolocker.*

[*] Öğr.Gör.Dr.Hacettepe Üniversitesi, Bilgisayar Mühendisliği, Bilişim Enstitüsü, karaikab@gmail.com
ORCID: 0000-0003-3700-4825

Geliş Tarihi / Received: 11.11.2018
Kabul Tarihi / Accepted: 12.12.2018

1.GİRİŞ

Tüm dünyada olduğu gibi, ülkemizde de son günlerde fidye yazılım saldırıları hızla artmaya başlamıştır (Shen vd., 2018:1; Feizollah vd., 2017:65). Her geçen gün daha fazla kullanıcıyı etkileyen bu zararlı yazılımlar, kullanıcıların zaman ve maddi kayba uğramasına neden olmaktadır (Rieck vd., 2011:640). Saldırganlar, fidye yazılım yoluyla kullanıcıların sisteminde bulunan dosyaları şifrelemekte daha sonra ise şifrelerin çözümü için fidye talep etmektedir. Hedef sisteme sızmak için en yaygın kullandıkları yöntem, kullanıcılara e-postalar göndermek ve e-posta ekinde bulunan zararlı yazılımı sistemlerine kurmak için yönlendirmektir (Bassett vd., 2006:1; Kara., 2015:87; Rieck vd., 2011:641).

Bu yöntemde, kullanıcıya oltalama yöntemini kullanılarak tasarlanmış bir e-posta içeriği gönderilmektedir. İlk bakışta resmi bir kurumdan gelen bir belge gibi görünen içerik, kullanıcının dikkatini çekmek ve onu korkutmak için özel olarak tasarlanmıştır. Burada amaç kullanıcının e-posta ekinde bulunan .exe uzantılı zararlı yazılımı aktif hale getirmesini sağlamaktır. Kullanıcı bu dosyayı çalıştırdığı andan itibaren zararlı yazılım hedef sistemde aktif olmaya başlamakta ve sistemin alt katmanına yerleşip, dosyayı şifrelemektedir (Yaqoob vd., 2017:444).

Hedef sistemde aktif hale gelen zararlı yazılım ilk olarak kendini rastgele isimlerle C:/Windows/ dizininin içine kopyalamaktadır (Luo ve Liao, 2007:196). Sistem her açıldığında otomatik olarak aktif hale gelebilmek için sistemin kayıt defterinde bir anahtar girdisi oluşturmaktadır (Bhardwaj vd., 2016:2). Bu aşamalardan sonra zararlı yazılım hedefteki tüm dosyaları şifrelemektedir (Richardson ve North, 2017:11).

Son günlerde ülkemizde sıklıkla görülmeye başlanan TeslaCrypt fidye yazılımı oldukça tehlikeli yeni nesil fidye yazılımdır (Garg vd., 2018:245). TeslaCrypt fidye yazılımlarının ilk sürümleri özellikle oyun dosyaları üzerinde etkili olmuş, oyun kartları ve oyuncu profilleri gibi dosyaları hedef almıştır (Salz vd., 2003;12). Güncellenen sürümlerde şifreleme kapasitesi daha da artmıştır. TeslaCrypt fidye yazılım, hedef sistemdeki dosyaları şifrelendikten sonra kullanıcıya, dosyaların şifrelendiğini bildiren bir mesaj göndermekte, şifrelerin çözümü içinse bitcoin eşdeğer miktarda 500$ veya € ödeme istemektedir (Villeneuve, 2015:13). Bu davranışları ile en çok bilinen fidye yazılım olan Cryptolocker (kripto kitleyicilere) ile çok benzemektedir (Zheng vd., 2017:313).

2. TESLACRYPT NASIL BULAŞIR?

TeslaCrypt fidye yazılımın hedef sistemlere sızma yöntemlerini genel olarak şöyle sıralanabilir;

- e-posta içeriğinde bulunan .exe uzantısı ile,
- Ücretsiz paylaşım sitelerinden (Torrent'ler gibi) indirilen oyun, film, müzik dosyaları ile,
- Uzak Masaüstü erişimi (RDP) ya da diğer sistem açıklıklarını kullanarak,
- Ücretsiz çevrimiçi film, dizi izleme bloklarını kullanabilmek için flash/java gibi programların eklentilerinin indirilmesiyle,
- Resmi olduğu düşünülen, siber suçlular tarafından modifiye edilerek değiştirilen kaynaklardan indirilen uygulamalar ile,
- Sosyal paylaşım blogları, haber ve ilan sitelerinin ziyaretleri sırasında (istemsiz), hedef sisteme sızmakatadır.

TeslaCrypt fidye yazılımı, AES (Advanced Encryption Standard) şifreleme yönteminde 256-bit standart bir algoritma kullanmaktadır. AES şifrelemesi, Amerikan hükûmeti tarafından uluslararası alanda da defacto şifreleme standardı olarak kullanılmaktadır (Aurangzeb, 2017:2).

TeslaCrypt fidye yazılım tehdidinden kurtulmak ve bu yazılım ile etkin bir mücadele geliştirmek için öncelikle tehditin detaylı tanımlanması gerekmektedir. TeslaCrypt'ların hedef

sisteme sızma ve dosyaları şifreleme işlemi sırasında kullandığı yöntemlere yönelik uygulamalı çalışmalar, problemin çözümünde önemli katkılar sağlayabilir.

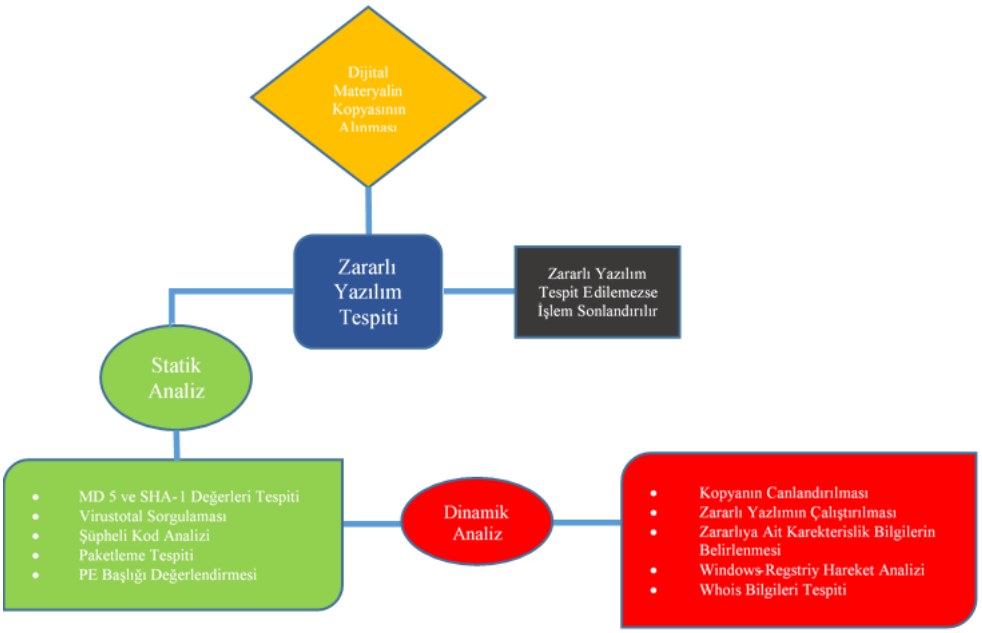
Bu çalışmada, yeni nesil TeslaCrypt fidye yazılımın hedef sistemde tespiti edilmesi, sisteme sızması ve dosyaları şifreleme davranışları detaylı olarak incelenmiş olup çalışma sonunda şifrelenen dosyalar başarılı şekilde kurtarılmıştır.

3. METOT ve BULGULAR

Zararlı yazılım analizleri için standart olarak uygulanan bir metod bulunmamaktadır. Bununla beraber ilk olarak zararlı yazılım çalıştırmadan yapılan statik analiz, ikinci olarak konrtollü bir ortamda zararlı yazılımı çalıştırarak yapılan davranış hareketlerinin (dosya-dizin hareketleri) analiz edildiği dinamik analiz ve son olarak ise zararlı yazılımın sahip olduğu mimarinin analizi için kod analizi yapılmaktadır. Zararlı yazılımın bulunduğu kurban bilgisayarda (canlı sistemde) kontrolün zor olması, zararın daha büyük boyutlara ulaşması gibi kötü senaryolar nedeniyle prensip olarak inceleme yapılamamaktadır. Bu nedenle kurban bilgisayar kopyası alınarak farklı bir ortamda (iş bilgisayarında) analizler yapılmaktadır.

TeslaCrypt fidye yazılım saldırısına maruz kalmış bilgisayarın, FTK Imager (free version) programı kullanarak kopyası alınmıştır. İncelenen TeslaCrypt fidye yazılımı çalıştırıldıktan sonra kullanıcı verilerine hızlı bir şekilde saldıracağından, inceleme yapılan iş makinesi sanal makine modunda çalıştırılmıştır. TeslaCrypt fidye yazılımının karakteristik davranış analizi için yapılan incelemeler "AccessData Forensic Toolkit v6.2.1.10 (FTK)", "Process Explorer" "Cuckoo" aracılığıyla gerçekleştirilmiştir.

Zararlı yazılım analizleri için standart olarak uygulanan bir metod olmamakla beraber genel eğilim basitten karmaşığa doğru ilerlemektedir. İlk olarak zararlı yazılım çalıştırılmadan elde edilebilecek tüm bilgilere ulaşmak daha sonra zararlı yazılımın kontrollü bir ortamda çalıştırılmasıyla davranış hareketlerini incelemek son olarak ise zararlı yazılımın kod mimarisinin incelenmesi doğru bir yöntem olacaktır. Bu çalışmada, analiz adımları için bir model önerilmiş ve önerilen model algoritması uygulanmıştır (Şekil 1).



Şekil 1. Önerilen zararlı yazılım analiz model algoritması.

Önerilen model algoritması doğrultusunda incelemelerde ilk olarak statik analiz yapılmıştır. Statik analiz sonucunda, TeslaCrypt fidye yazılımının bulunduğu kurban bilgisayara ait bilgiler FTK ve Process Explorer programları kullanılarak elde edilmiş olup Tablo 1 ve Tablo 2'de verilmiştir.

Tablo 1. Cihaz Bilgileri

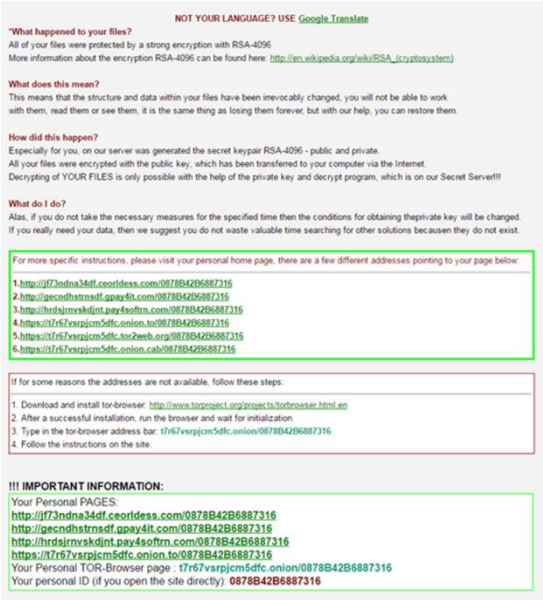
Açıklama	Physical Disk, 1.953.525.168 Sectors 931,5 GB
Toplam Kapasite	1.000.204.886.016 Bytes (931,5 GB)
Toplam Sektör	1.953.525.168
MD5 Değeri	5ebd653ee743d236356914173e8c6174
MD5 Doğrulama	5ebd653ee743d236356914173e8c6174
SHA1 Değeri	6f316c8a441fd83a6ee04caffbd87d1a3c715ab0
SHA1 Doğrulama	6f316c8a441fd83a6ee04caffbd87d1a3c715ab0

Tablo 2. İşletim Sistemi Bilgileri

Ürün Adı	Windows 7 Ultimate
Kayıtlı Sahip	user
Sistem Kökü	C:\Windows\
Güncel Veriyonu	6.1
CSD Versiyonu	Service Pack 1
Kurulum Tarihi	27.11.2015 11:55:39 UTC
Son Kapanma Tarihi	23.12.2015 10:57:10 UTC

Tablo 1 ve 2'de TeslaCrypt fidye yazılımının bulunduğu kurban bilgisayara ait bilgiler zararlı yazılım analizleri için gereklidir. Bu bilgilerden yolla çıkarak analiz için kullanılacak programlarının ilgili sürüm ve özellikleri seçilmektedir. Ayrıca buradan edinilen bilgiler zararlı yazılımın olası karekterislik hareketlerinin tahmin edilmesi sağlamaktadır.

Önerilen model algoritması doğrultusunda incelemelerin ikinci aşaması olarak dinamik analiz yapılmıştır. Dinamik analiz için alınan kopya çalıştırıldığında saldırgana ait olduğu anlaşılan mesaj kurban bilgisayarın ekranında görülmüştür (Şekil 2). Mesajdan da anlaşılacağı gibi saldırının nedeni "TeslaCrypt" fidye yazılımı olduğu tespit edilmiştir. Hedef sistemde aktif hale gelen TeslaCrypt fidye yazılıma ait ilk iz "IMAGE.E01/Partition 2/NONAME [VSC]/[Current]/[root]/Users/user/Desktop/" dizini altında bulunan "**Howto_Restore_FILES.HTM**" isimli dosya içerisinde Şekil 2'de verilen nota ulaşılmıştır. Bu aşamadan sonra incelemeler "Howto_Restore_FILES.HTM" dosyası üzerine yoğunlaştırılmıştır.

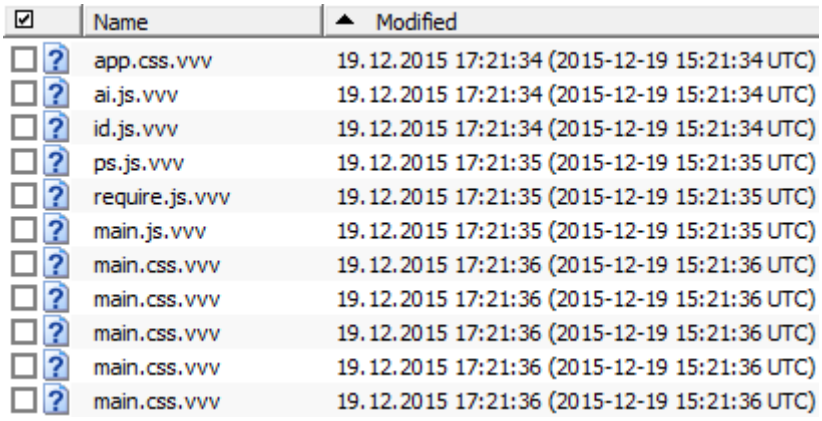


Şekil 2. Kurban bilgisayarda TeslaCrypt virüsün olduğu bildiren saldıgana ait mesaj.

Tablo 3. FTK ve Cuckoo programları kullanılarak elde edilen "Howto_Restore_FILES.HTM" dosyasına ait teknik bilgileri.

Dosya Bilgileri	
Dosya Adı	Howto_Restore_FILES.HTM
Oluşturma Zamanı	20.12.2015 13:57:55 (2015-12-20 11:57:55 UTC)
Erişim Zamanı	20.12.2015 13:57:55 (2015-12-20 11:57:55 UTC)
Değiştirme Zamanı	20.12.2015 13:57:55 (2015-12-20 11:57:55 UTC)
Dosya Boyutu (Byte)	10.631 bytes (10,38 KB)
MD5 Hash Değeri	83e36d32d8e26e55515437c4492d6270
Dosya Yolu	IMAGE.E01/Partition 2/NONAME [VSC]/[Current]/[root]/Users/user/Desktop/

TeslaCrypt fidye yazılımın hedef sistemdeki hangi dosyaları şifrelediğini tespit etmek için yapılan incelemelerde .vvv uzantısına sahip çok sayıda şifreli dosyanın varlığı tespit edilmiştir (Şekil 2).

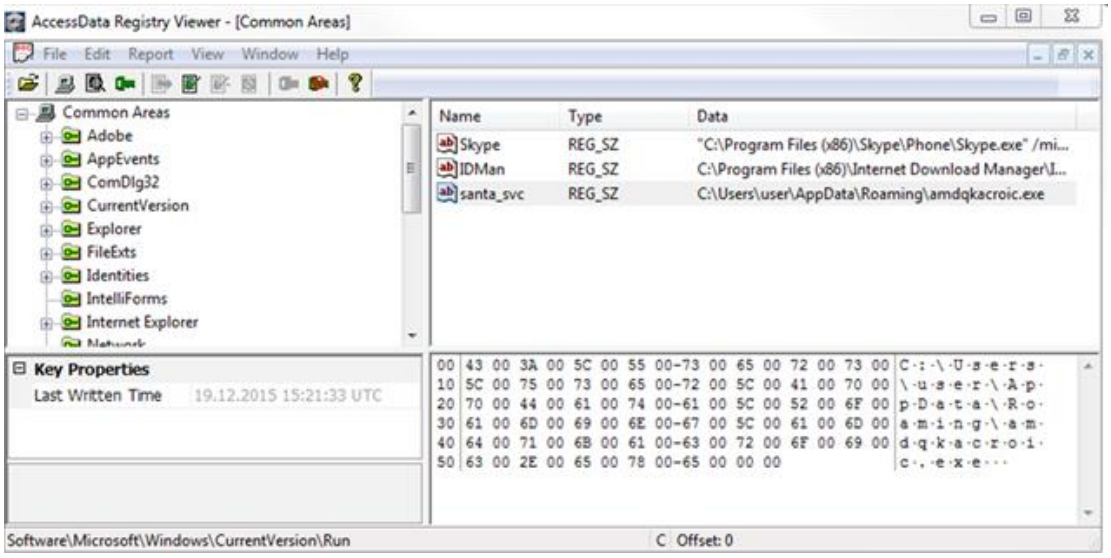


Şekil 3. Kurban bilgisayardaki dosyaların şifrelenmiş olduğunu gösteren ekran görüntüsü.

Kopya üzerinde yapılan incelemelerde dosya şifreleme işlemlerinin "19.12.2015 17:21:34 (2015-12-19 15:21:34 UTC)" zaman diliminde başladığının tespit edilmesi üzerine, bu tarihte çalıştırılan dosyalar üzerinde incelemeler gerçekleştirilmiştir. Yapılan incelemelerde olay günü "IMAGE.E01/Partition2/NONAME[VSC]/[Current]/[root]/Users/user/NTUSER.DAT»Software»Microsoft»Windows»CurrentVersion»Run»" altında bulunan registry kaydından "amdqkacroic.exe" (TeslaCrypt) isimli zararlı yazılım dosyaların şifrelendiği tespit edilmiştir (Şekil 3).

"amdqkacroic.exe" isimli zararlı yazılım araştırıldığında söz konusu zararlı yazılımın dosyaları şifreledikten sonra kendisini sildiği görülmüştür. Bu aşamadan sonra TeslaCrypt fidye yazılımının sebep olduğu şifrelenmiş dosyaların kurtarılması yönünde araştırmalar gerçekleştirilmiştir. Şifre kırmak için birçok yöntem olmakla beraber inceleme konusu TeslaCrypt fidye yazılımının çok güçlü bir şifreleme standartını kullandığı bilinmektedir. Bu nedenle brute-force (her olası harfleri, numaraları ve karakterleri doğru şifreyi bulana kadar denemek) yöntemini kullanmak mantıklı değildir. Çözümlenmiş fidye yazılımların şifrelerini içeren kelime listesi (word list) yöntemini kullanmak bazı durumlarda başarılı sonuçlar vermektedir.

Bu çalışmada şifrelenmiş dosyaları kurtarma işlemleri için "AccessData Registry Viewer" adlı program kullanılmıştır. AccessData Registry Viewer programı, windows işletim sistemi için AccessData tarafından geliştirilmiş ve FTK programı ile ilişkili olarak çalıştırılmaktadır. Önceden hazırlanmış word list ile yapılan analizler sonucunda şifrelenmiş dosyalar başarılı şekilde kurtarılmıştır (Şekil 4).



Şekil 4. "amdqkacroic.exe "isimli zararlı yazılımın çalıştırıldığına ait ekran kaydı.

4. SONUÇLAR VE DEĞERLENDİRME

Her geçen gün yeni tasarımlar ile piyasaya sürülen zararlı yazılımlar tüm kullanıcılar için giderek büyüyen bir tehlike haline gelmiştir. Fidye yazılımlar hedef sisteme sızdıktan sonra sistemde bulunan dosyaları şifrelemekte, dosyalara tekrar erişim sağlanmak için gerekli anahtarı alma karşılığında ise saldırgana fidye ödenmesini talep etmektedir.

TeslaCrypt, yeni nesil fidye yazılım türlerinden birisidir. Sanal ortamda her gün yayılmaya devam etmekte ve birçok kullanıcının başına bela olmaktadır. Saldırganlar, TeslaCrypt fidye yazılımı ile daha ziyade küçük işletmeleri ve şirketleri hedef almaktadır. Son günlerde artan saldırılar sonucunda, TeslaCrypt fidye yazılımından etkilenen kullanıcı sayısında ciddi artışlar

görülmüştür. Bu nedenle gerçek bir olaydan alınan TeslaCrypt fidye yazılım saldırısı detaylı olarak incelenmiştir. Bu alanda yapılan çalışmalara teknik analiz boyutunun gerekli olduğu sunulmuştur. Tespiti yapılan TeslaCrypt fidye yazılımının şifrelediği dosyalar üzerinde yapılan incelemeler tamamlandıktan sonra, şifrelenen dosyalar başarılı şekilde kurtarılmıştır.

İşletmelerin, kişilerin aleyhlerine giderek sıklaşan ve giderek daha tehlikeli hale gelen kötü niyetli saldırılara karşı, güvenlik tehditlerini ve zaafları ortadan kaldıran kapsamlı bir çözüm gereksinimleri vardır. Fidye yazılımlar tarafından şifrelenmiş dosyalar erişimi engellendiği için temel olarak onarılamaz kabul edilmektedir. Bu nedenle fidye yazılımların saldırılarına maruz kalmamak için bir takım tedbirler alınması gereklidir. Fidye yazılım saldırılara karşı alınması gereken önlemler şu şekilde önerilebilir;

i. Fidye yazılımlar en yaygın sızma yöntemi e-posta yolunu kullanmaktadır. Bu nedenle kaynağından emin olunmayan bu gibi sahte e-postaların içindeki sahte faturaları açmamak.
ii. Kullanıcı e-mail sistemlerine AntiSpam ürünlerini kullanmak,
iii. Kullanıcılara fatura, haciz, kargo bilgileri gibi e-faturanın zip formatında veya exe formatında olmayacağını farkındalığının oluşturmak
iv. Herkes tarafından kabul gören güncel bir Internet Security yazılımı ile sistemleri koruma altına almak,
v. Uzaktan erişim portunu değiştirmek (mümkünse port numarası uzun karakterlerden oluşturmak), uzaktan erişen kullanıcılara kısıtlı hesaplar ve güçlü şifreler oluşturmak ve kullanılmayacaksa uzaktan erişime sisteme kapatmak,
vi. Daha önce tespit edilen fidye yazılım alanlarına girişleri bloke etmek,
vii. Kullanıcının önemli verilerini başka bir depolama sisteminde günlük yedek almak (En az 30 günlük "geri yükleme noktaları" oluşturmak).

Bu ve benzeri önlemleri alarak kesin olarak fidye yazılımlardan korunmamakla birlikte kullanıcılar için farkındalık oluşturması açısından önemlidir. Araştırmanın yalnızca siber güvenlik endüstrisi üzerinde değil, yakın gelecekte yapılacak araştırmalarda ve birçok bireysel internet kullanıcısnın üzerinde de olumlu bir etki yaratmasını beklenmektedir.

KAYNAKÇA

Aloul, F. A. (2012). The need for effective information security awareness. Journal of Advances in Information Technology, 3(3), 176-183.

Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017). Ransomware: A Survey and Trends. Journal of Information Assurance & Security, 6(2).

Bassett, R., Bass, L., & O'Brien, P. (2006). Computer forensics: An essential ingredient for cyber security. Journal of Information Science & Technology, 3(1).

Bhardwaj, A., Avasthi, V., Sastry, H., & Subrahmanyam, G. V. B. (2016). Ransomware digital extortion: a rising new age threat. Indian Journal of Science and Technology, 9(14), 1-5.

Feizollah, A., Anuar, N. B., Salleh, R., Suarez-Tangil, G., & Furnell, S. (2017). Androdialysis: Analysis of android intent effectiveness in malware detection. computers & security, 65, 121-134.

Garg, D., Thakral, A., Nalwa, T., & Choudhury, T. (2018). A Past Examination and Future Expectation: Ransomware. In 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE) (pp. 243-247). IEEE.

Kara, İ., (2015). Türkiye de Zararlı Yazılımlarla Mücadelenin Uygulama Ve Hukuki Boyutunun Değerlendirilmesi. Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi 52: 87-98.

Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. Information Systems Security, 16(4), 195-202.

Salz, J., Balakrishnan, H., & Snoeren, A. C. (2003). TESLA: A Transparent, Extensible Session-Layer Architecture for End-to-end Network Services. In USENIX Symposium on Internet Technologies and Systems.

Shen, J., Gong, S., & Bao, W. (2018). Analysis of Network Security in Daily Life. Information and Computer Security, 1(1).

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10-21.

Rieck, K., Trinius, P., Willems, C., & Holz, T. (2011). Automatic analysis of malware behavior using machine learning. Journal of Computer Security, 19(4), 639-668.

Villeneuve, N. (2015). TeslaCrypt: Following the Money Trail and Learning the Human Costs of Ransomware. Threat Research Blog.

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 129, 444-458.

Zheng, B., Zhu, L., Shen, M., Du, X., Yang, J., Gao, F., ... & Yin, S. (2017). Malicious Bitcoin Transaction Tracing Using Incidence Relation Clustering. In International Conference on Mobile Networks and Management (pp. 313-323). Springer, Cham.