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

İNTERPOL FİDYE YAZILIM SALDIRISI VE ANALİZİ

İlker KARA[1]

[1] Hacettepe Üniversitesi, Bilişim Enstitüsü, Yapı Eğitimi Bölümü, 06800, Ankara, TÜRKİYE
karaikab@gmail.com.

Özet-Bu çalışma; İnterpol fidye yazılım virüsünün teknik analizini içermektedir. Fidye yazılımlar, kişisel kullanıcılar ve kurumlara ait sistemlere çeşitli yöntemlerle sızarak sistemde bulunan dosyaları şifreleyen, şifrelediği dosyaları kullanıcının tekrar erişimine açmak için mağdurlardan fidye isteyen zararlı yazılımlardır. Alınan tüm tedbirlere rağmen dünya genelinde yapılan fidye yazılım saldırıların sayısı her geçen gün artmaktadır. Son günlerde Avrupa ve Kuzey Amerika ülkelerini hedef alan yeni bir tür fidye yazılımı olan "İnterpol fidye yazılım" virüsü olarak adlandırılan siber saldırılar ülkemizde de görülmeye başlamıştır. Bu çalışmanın amacı, İnterpol fidye yazılım virüsüne yaklaşım ve teknik analiz yapılarak bu tehdide karşı farkındalık oluşturulması hedeflenmiştir.

Anahtar Kelimeler- Siber Güvenlik, Zararlı Yazılımlar, İnterpol Fidye Yazılımı.

INTERPOL RANSOMWARE ATTACTK AND ANALYSİS

Abstract-This study addresses technical analysis of the Interpol ransomware virus. Ransomware malware infiltrate the systems belonging to personal users and institutions via various techniques, encrypt files in the system and request ransom from the victim to allow access to the encrypted files. Despite all the measures taken, the number of ransomware attacks is increasing across the globe every passing day. A new kind of cyberattacks, called "Interpol ransomware" virus, which is a new kind of ransom software targeting European and North American countries, have started to be seen in Turkey recently. Hence, this study aims to detect and analyze the Interpol ransomware virus in order to raise awareness among against this threat.

Key Words- Cyber Security, Malware, Interpol Ransomware.

1. GİRİŞ (INTRODUCTION)

Geçmişteki siber saldırılar; bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirmeye yönelik tasarlanırken, günümüzde daha çok mağdurlardan fidye almaya yönelik saldırılara dönüşmüştür [1]. Bu amaç için özel olarak tasarlanmış zararlı yazılımlar, kullanıcıların maddi kayıplarının yanı sıra, itibar, müşteri ve pazar kaybı sorunlarına neden olmaktadır [2, 3].

Fidye yazılımlar, bulaştıkları sistemi tamamen ya da sistemde bulunan bazı dosyaları şifreleyerek şifrenin kaldırılması için kullanıcıdan fidye talep eden zararlı yazılımlardır [4]. Son yıllarda dünya genelinde görülen bu zararlı yazılımlar, yerel dil, bölgesel kurumlar vb. nedenlerle uygulandığı bölgelere göre farklılıklar göstermektedir. Bu tehditten korunmak için alınan tedbirler yetersiz

kalmakta ve alınan tüm güvenlik önlemlerine rağmen her geçen gün bu saldırıya maruz kalan kullanıcı sayısı artmaktadır [5]. Birçok saldırı yöntemi kullanan bu zararlı yazılımlar, genellikle ilk bakışta zararsız gibi görülen bir e-posta ekinin açılması ya da içeriği değiştirilmiş bir internet sitesinden kullanıcıların sistemine sızılmasıyla gerçekleşmektedir [6].
Geliştirilen anti virüs programları ve benzer sandbox'lar (kum havuzu) bu tehditle etkin mücadele etse de tam olarak başarı sağlanamamıştır [7]. Son günlerde ülkemizin de içinde bulunduğu Avrupa ve Kuzey Amerika ülkelerinde görülmeye başlayan yeni bir tür fidye yazılım; kullanıcılara mesaj ile ulaşarak kolluk kuvveti veya uluslararası güvenlik yetkilisi tarafından gönderilmiş gibi görülen ve kullanıcının sisteminde çocuk pornografisi veya başka bir yasadışı içerik bulunduğunu iddia eden bir yazılımdır [8]. Gönderilen bu mesajla birlikte kullanıcının ceza olarak fidye ödemesi istenmektedir. Saldırganlar, korkutma taktiğini kullandıkları bu yöntemle kullanıcıları paniğe sevk ederek son derece etkili ve kolay bir şekilde kullanıcıdan fidye alabilmektedirler [9].

2. FİDYE YAZILIM TÜRLERİ NELERDİR? (WHAT ARE THE RANSOMWARE TYPES?)

Fidye yazılımlar, genel olarak iki kategoriye ayrılmaktadır[10]. Bunlar:

i) Şifreleyiciler fidye yazılımlar,
ii) ii) Kilitleyici fidye yazılımlar.

2.1. Şifreleyici Fidye Yazılımları (Encryption Ransomware)

Şifreleyici fidye yazılımları, hedef sisteme sızdıktan sonra sistemde bulunan tüm veri dosyalarını (ofis dosyaları, sistem dosyaları, oyun dosyaları, fotoğraflar vb.) şifrelemektedir. Şifreleme yapıldıktan sonra saldırgan tarafından mağdura, yapılan işlem ve dosyalara tekrar erişebilmek için bir bilgi mesajı gönderilmektedir. Bilgi mesajında; dosya içeriklerine erişimin yalnızca özel anahtar ile açılabileceği, bu anahtarı alabilmek için fidye ödenmesinin zorunlu olduğu belirtilmektedir. Fidyenin, bitcoin (kripto para) veya Ukash PIN (sanal para) ile ödenmesi istenmektedir. Fidye miktarı, genellikle 300$ civarındadır [11-14].

2.2. Kilitleyici Fidye Yazılımları (Loc ker Ransomware)

Kilitleyici fidye yazılımları, diğer kategoriden farklı olarak belirli dosyaları değil tüm sistemi kilitleyerek kullanılmaz hale getirmektedir. Ancak kişisel dosyalar şifrelenmemektedir [15] (Kharraz, 2015:4) Hedef sisteme bulaştıktan sonra ana ekranda saldırgana ait bir mesaj görünmektedir. Bu mesaj, sistemin tekrar kullanıma açılması için fidye ödenmesi gerektiğini içermektedir.

Ukash virüs ailesinin son sürümü olan Interpol fidye virüsü, ilk olarak Avrupa ve Kuzey Amerika ülkelerini hedef almıştır [15-18]. Son günlerde ülkemizde de görülmeye başlayan Interpol fidye virüsü, bilgisayarlarda bulunan dosyaları şifrelemektedir [19,20]. Şifrelemenin kullanıcının yasa dışı bir erişim yapması nedeniyle güvenlik güçleri tarafından yapıldığını bildiren bir mesaj kurbana iletilmektedir. Saldırgan, kurbanı panik ve korkuya sevk ederek saldırgana talimatlarını yerine getirmesini amaçlamaktadır.

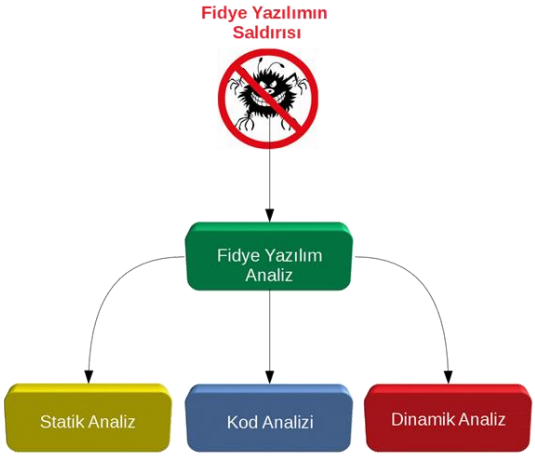
İnterpol fidye yazılım saldırılarından korunmak için öncelikle tehdit unsurunun detaylı olarak tanımlanması gerekmektedir. Hedef sistemlere sızma yöntemleri, saldırı anında hedef sistemdeki hareketlerin tespitine yönelik uygulamalı çalışmalar, fidye yazılımlarla etkin mücadeleye önemli ölçüde katkı sağlayacaktır.

Bu çalışmada, İnterpol fidye yazılımın kurban sistemde tespiti, sisteme sızması ve zararlı yazılımının bulunduğu web sitenizin teknik analizi detaylı olarak incelenmiştir.

3. ÖRNEK OLAY İNCELEMESİ (CASE STUDY)

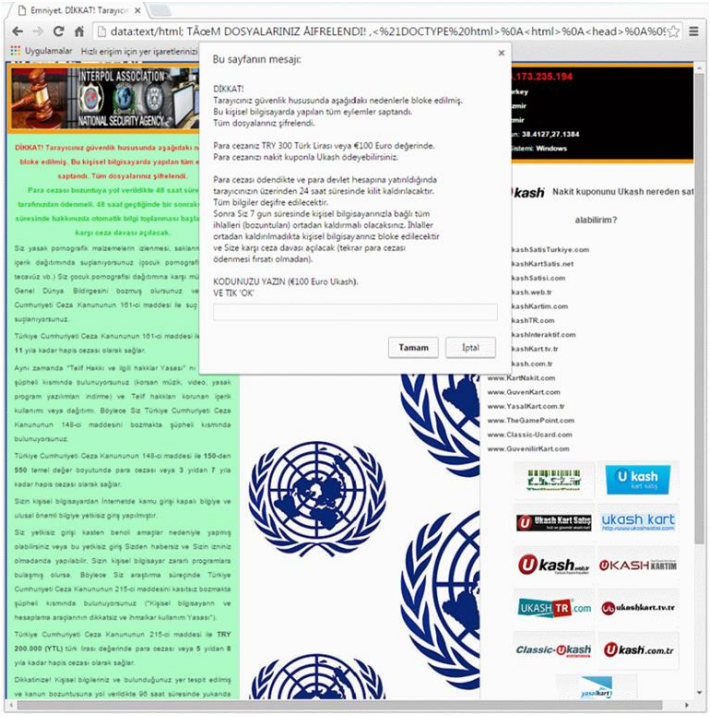
İnterpol fidye yazılımın saldırısına uğramış kurban bilgisayarın incelemesi, ilk olarak zararlı yazılımın tespit edilmesiyle başlamaktadır [8]. Tespiti yapılan fidye yazılım çalıştırmadan hakkında elde edilebilmek için statik analiz yapılmaktadır [3]. Dinamik analiz, zararlı yazılımın çalıştırılarak sistemdeki etkileri ve aktivitelerini (dosya-dizin hareketleri) tespit etmek için yapılmaktadır [4]. Kod analizi ise, Statik ve dinamik analiz sonucunda elde edilen kod mimarisini analizi ve yorumlanması yapılmaktadır (Şekil 1).

Tespit edilen İnterpol fidye yazılımın teknik analizi için yapılan incelemelerde uzmanlar tarafından en çok tercih edilen "AccessData Forensic Toolkit v6.2.1.10 (FTK)", "Process Explorer" "Wireshark", "Cuckoo" programları kullanılmıştır. Seçilen örnek olay gerçek bir siber saldırı olduğundan, tespit edilen veriler gizlenerek çalışmada sunulmuştur.



Şekil 1. Fidye yazılım analiz yöntemi (Ransomware analysis method)

Kurban bilgisayarda zararlı yazılım tespiti amacıyla son yapılan işlemler incelendiğinde 25.10.2018 günü saat 14:05 sıralarında bilgisayarın ana ekranında "İnterpol tarafından, çocuk pornosu ve vizesiz gazete çoğaltmak suçlarından aranıldığından dolayı sistemde bulunan tüm dosyaların şifrelendiği ceza olarak ta 300 TL ya da 100 Euro ödemesini cezanın ödenmediği takdirde istinat edilen suçlardan, müştekinin mahkemeye verileceğini" belirten mesajın içeriğinden İnterpol fidye yazılım virüsünün olabileceği değerlendirilmiştir (Şekil 2).



Şekil 2. İnterpol fidye zararlı yazılımına ait ekran görüntüsü (Screenshot of Interpol Ransomware)

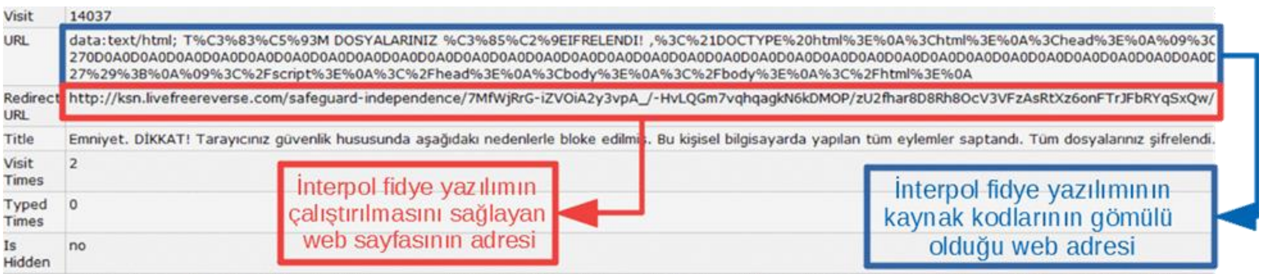
Zararlı yazılımın tespiti yapıldıktan sonra kurban bilgisayarda zararlı yazılıma ait incelemeler yapılmıştır. Saldırganlar, hedef sisteme sızmak için en çok kullandığı yöntem içeriği değiştirilmiş e-posta ile ulaşarak ekinde bulunan zararlı yazılımın içinde gömülü olduğu çalıştırılabilir .exe'yi kullanıcının sisteme yüklemesi için yönlendirmektedir. Yapılan incelemelerde kurban bilgisayarda çalıştırılabilir (.exe uzantısına sahip) her hangi bir zararlı yazılıma rastlanılmamıştır.

Saldırganın kurban sisteme sızmak için kullandığı başka bir yöntem ise tahrip edilmiş internet sitesi üzerinden çevrimiçi olarak yaptığı saldırılardır. Kurban bilgisayarının internet kayıtları üzerinde yapılan incelemelerde; "Avast Antivirüs" yazılımının kullandığı"k15_390.image.001\Partition2\NONAMENTFS]\[root]\Users\user\AppData\Local\Temp\avastBCLTMP\chrome\Default\" dizininde bulunan "Google Chrome" isimli web tarayıcısına ait "history" isimli sqlite dosyası içeriğinde bulunan "0014037" isimli kayıtta "http://ksn.livefreereverse.com/safeguardindependence/7MfWjRrGiZVOiA2y3vpA_HvLQGm7vqhqagkN6kDMOP/zU2fhar8D8Rh8OcV3VFzAsRtXz6onFTrJFbRYqSxQw/tTNFwdRIPMosUQBUxFFtfanMv7idoBkDP4GCxokik/case-law.jsp" linki üzerinden yönlendirme yapılarak İnterpol fidye yazılımının çalıştırıldığı tespit edilmiştir.

İnterpol fidye yazılımına ait teknik bilgi Tablo 1'de verilmiştir.

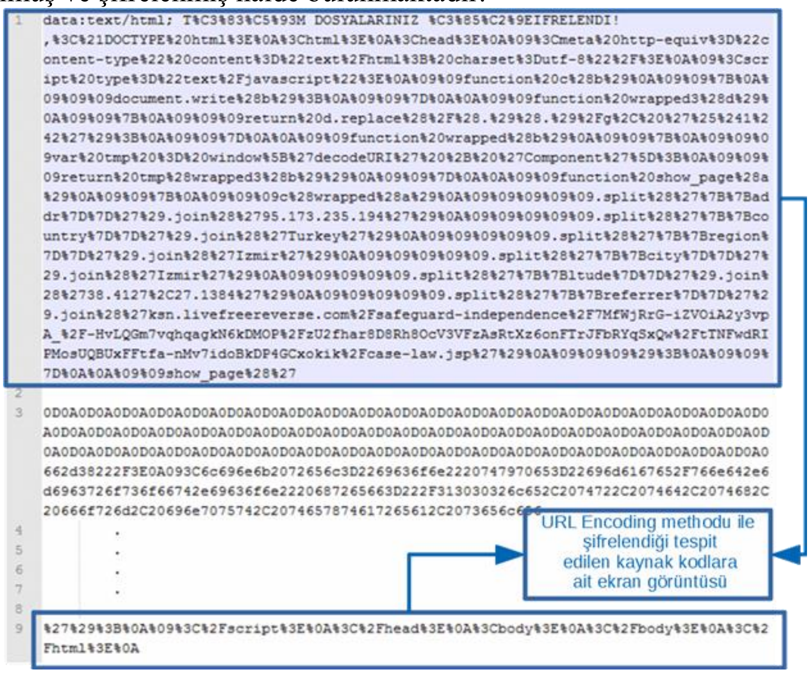
Tablo 1. Statik analiz sonucu İnterpol fidye yazılımına ait teknik bilgiler (Technical data of Interpol ransomware as a result of static analysis)

Dosya Bilgileri	
Dosya Adı	**history**
Oluşturma Zamanı	26.10.2018 10:08:31 (2018-10-26 07:08:31 UTC)
Son Erişim Zamanı	26.10.2018 10:08:31 (2018-10-26 07:08:31 UTC)
Değiştirme Zamanı	13.12.2018 00:38:39 (2018-12-12 21:38:39 UTC)
Dosya Boyutu (Byte)	12.783.616 bytes (12,19 MB)
MD5 Hash Değeri	135c69a4ca1564e7c8ea006dfda39c85
Dosya Yolu	k15_390.image.001\Partition 2\NONAME [NTFS]\[root]\Users\user\AppData\Local\Temp\avastBCLTMP\chrome\Default\History



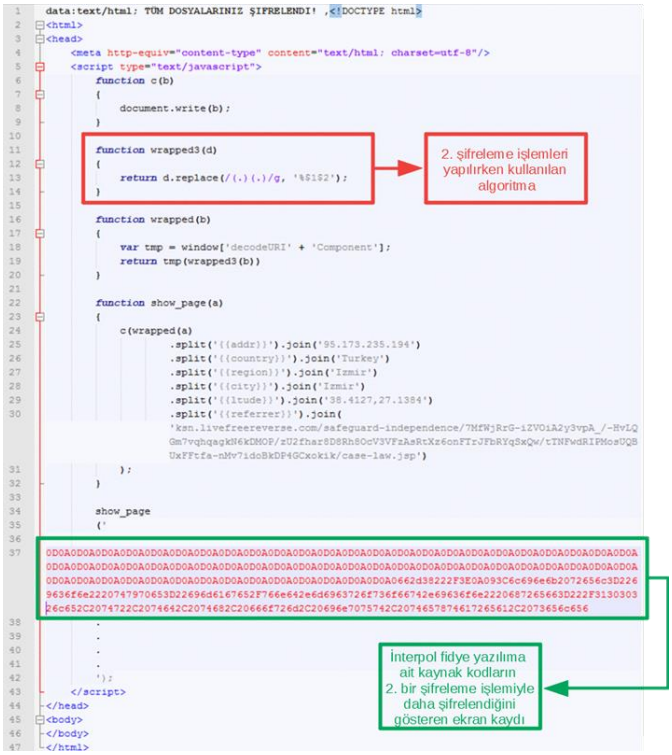
Şekil 3. Google Chrome "history" dosyası içeriğinde bulunan "14037" nolu kayıtları (Google Chrome records "14037" in the "history" file content)

Google Chrome "history" dosyası içeriğinde bulunan "14037" nolu kayıtların Şekil 2' de verilmiştir. Şekil 2'den görülebileceği gibi İnterpol fidye yazılımına ait kaynak kodlar link üzerine gömülmüş ve şifrelenmiş halde bulunmaktadır.



Şekil 4. "URL dil kodlaması (Encoding)" metodu kullanılarak şifrelenmiş kaynak kodlara ait ekran görüntüsü (Screenshot of encrypted source code using the "URL language Encoding" method)

Şekil 4'de detaylı bilgileri verilen URL Encoding metodu ile şifrelendiği tespit edilen zararlı yazılıma ait kaynak kodlar "http://www.danstools.com/" web adresi üzerinden çözümlenmiş ve Şekil 5'te bilgisi verilen kaynak kodlara ulaşılmıştır.



Şekil 5. "http://www.danstools.com/" web adresi üzerinden çözümlenmiş kaynak kodlara ait ekran görüntüsü ("http://www.danstools.com/" screenshot of the source code resolved over the web address)

Şekil 5'de bilgisi verilen ve kaynak kodlarının bir kısmının URL Encoding metodu ile şifrelenmiş olan İnterpol fidye yazılımının kaynak kodları çözümlendiğinde "javascript" dilini kullandığı tespit edilmiştir. Saldırgan bu dili kullanarak kaynak kodların bir kısmında ikinci defa şifrelenmektedir. Kaynak kodlar üzerinde yapılan incelemelerde ikinci şifreleme işleminin nasıl yapıldığı kodlar üzerinde yapılan incelemede tespit edilmiştir (Şekil 6). Çözümlemesi yapılan kaynak kodların "decoded.txt" isimli dosya içerisine eklenmiş olduğu tespit edilmiştir.

Şekil 6. "decoded.txt" isimli dosyaya ait ekran görüntüsü ("decoded.screenshot of the file named txt")

Şekil 6'de URL Encoding metodu ve saldırgana ait başka bir algoritmayla iki kez şifrelenmiş olan İnterpol fidye yazılımına ait kaynak kodların çözümlenmiş halini gösteren ekran görüntüsü örneği verilmiştir.

Şekil 6'de bilgisi verilen, İnterpol fidye yazılımına ait kodların tüm çözümleme işlemleri tamamlandığında saldırganın kurbanlardan ödemeyi Ukash PIN kodu ile yapmasını istediği tespit edilmiştir (Şekil 7). Saldırgana ait Ukash PIN kodu kullanılarak saldırganın hesap bilgilerine ulaşılabileceği ihtimali nedeniyle incelemeler bu alanda yoğunlaştırılmıştır.

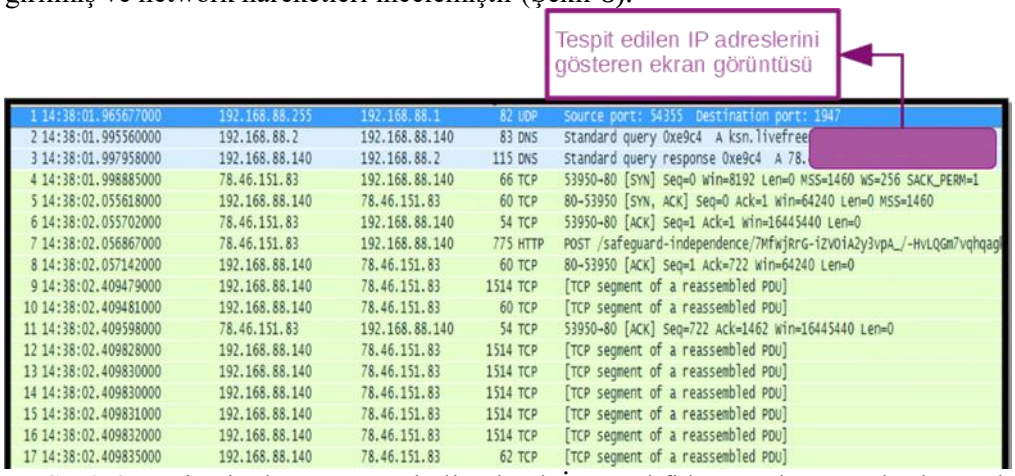
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "
http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
    <title>Emniyet. DİKKAT! Tarayıcınız güvenlik hususunda aşağıdaki nedenlerle
    bloke edilmiş. Bu kişisel bilgisayarda yapılan tüm eylemler saptandı. Tüm
    dosyalarınız şifrelendi. Siz yasak pornografik malzemelerin izlenmesi,
    saklanması veya içerik dağıtımında suçlanıyorsunuz (çocuk pornografisi,
    zoofili, tecavüz vb.) Siz çocuk pornografisi dağıtımına karşı mücadelenin
    Genel Dünya Bildirgesini bozmuş olursunuz ve Türkiye Cumhuriyeti Ceza
    Kanununun 161-ci maddesi ile suç işlemekte suçlanıyorsunuz.</title>


    <meta name="msapplication-config" content="none"/>
    <meta http-equiv="content-type" content="text/html; charset=utf-8"/>
    <link rel="icon" type="image/vnd.microsoft.icon" href="/1002/favicon.ico"/>

                    <style type="text/css">
                html, body, p, h1, h2, h3, h4, h5, em, i, table, tr, td, th,
                form, input, textarea, select, li, ol, ul, strong {padding:0;
                margin:0;}
html {font-size:62.5%;}
body {background:#ffffff url(../img/a_back0.jpg); color:#333333; font-size:10px;
font-family:Arial, Helvetica, sans-serif; min-width:1000px; line-height: 20px;}
em, i {font-style:normal;}
li {list-style-type:none;}
h1, h3, h4, h5 {font-weight:normal; padding:5px 0;}
h2 {font-weight:bold; font-size:12px; color:#000080; text-align:center;}
p {padding:2px 0; font-size:10px; text-align:justify;}
a:active, a:focus, img, input, select {outline:0;}
a, a:link, a:active, a:visited {color:#cc0000; cursor:pointer;
text-decoration:none;}
a:hover {color:#000000; text-decoration:underline;}
img {border:none;}
.clear {clear:both; font-size:0; line-height:0; height:0;}
strong {
    font-weight: bold
}

h1, h2, h3, h4, h5, h6 {
    margin: 10px 0;
    font-family: inherit;
    font-weight: bold;
    line-height: 20px;
    color: inherit;
    text-rendering: optimizelegibility
```

Şekil 7. Saldırgana ait Ukash PIN kodu örneği (An example of the attacker'S Ukash PIN code)

Saldırganın belirttiği Ukash PIN kodu örneği üzerinde yapılan incelemelerde, Ukash kodunun "633718" ile başlayıp [0-9] aralığında 13 haneli bir kod ile devam etmesi gerektiği görülmüştür (Örneğin: "6337181234567891234"). Mağdur ödeme sekmesine bu kod yapısına uygun bir kod girdiğinde saldırganın internet alanına gönderdiği görülmüştür. Farklı bir formatta kod ödeme penceresine giriş yapıldığında ise yanlış kod girildiğini belirten bir mesajın ekrana açıldığı görülmüştür.

Şekil 8. Kullanıcılardan alınan Ukash kodunun yapısını belirten kod örneği (Code sample that specifies the structure of the Ukash code received from users)

Saldırgana ait internet alanının IP (İnternet Protokol) adresine ulaşabilmek amacıyla, saldırganın belirtmiş olduğu yapıya uygun bir Ukash PIN kodu ile ödeme alanına bir kod örneği rastgele girilmiş ve network hareketleri incelemiştir (Şekil-8).



Şekil 9. "Wireshark" programı kullanılarak İnterpol fidye yazılımına Ukash PIN kodunun analizi (Analysis of Ukash PIN code for Interpol ransom software using the "Wireshark" program)

Şekil 8'den İnterpol fidye yazılımına ait network hareketleri "Wireshark" programı kullanılarak analiz edilmiştir. Analizler sonucunda kurbanlardan talep edilen fidyeyi ödemesi için Ukash kodunu "ksv.livefrxxxxxyyyy.com" alan adına sahip "78.4X.1X1.8X ve 4X.4.XX0.1X3" IP adreslerine gönderdiği tespit edilmiştir. Tespiti yapılan IP adreslerine ve alan adına (domain name) ait WHOIS kayıtları "www.domaintools.com" adresi üzerinden sorgulanmış ve sorgulama sonucu saldırgana ait iletişim bilgilerine ulaşılabilir olduğu görülmüştür.

4. SONUÇ VE TARTIŞMA (CONCULUSION AND DISCUSSION)

Maddi kazanç, siyasi faaliyetler, bilgi casusluğu ve ülkelerarası siber terörizm gibi etkenler amacıyla zararlı yazılımlar üretilmektedir. Her geçen gün geliştirilen ve yeni türleri üreten zararlı yazılımların kullanıcılara verdikleri maddi kayıpları tüm zamanların en yüksek seviyesine ulaştığı görülmektedir. Fidye yazılımlar, getirdiği yüksek maddi getirisi nedeniyle en çok tercih edilen zararlı yazılım türüdür.

Son zamanlarda ülkemizin de arasında bulunduğu Avrupa ve Kuzey Amerika ülkelerini hedef alan İnterpol fidye yazılım virüs saldırılarında ciddi artış görülmektedir. İnterpol fidye yazılımı, saldırı ve sızma yöntemleri diğer fidye yazılımlarla farklılıklar göstermektedir. Temel olarak farklılıklar;

- En çok kullanılan yöntem olan hedef sisteme sızma (çalıştırılabilir - .exe uzantılı dosyalar) bu saldırıda kullanılmamıştır. Bunun yerine hedef sistem tahrip edilmiş bir internet sitesine yönlendirilmektedir. Bu alışıla gelmemiş durum analizciler için zorluk oluşturmaktadır. Çünkü zararlı yazılımın tespiti ve analizi için şüpheli internet sitesinin tespit edilmesi ve çevrimiçi olarak analiz yapılması gerekmektedir.

- Saldırganlara fidye ödeme şekli genel olarak kripto para birimi olan bitcoin olarak istenmektedir. Bu saldırıdaki ödemenin, daha az bilinen sanal para birimi olan Ukash PIN kodu ile yapılması istenmiştir.

- Saldırganlar, amaçlarına ulaşmak için içeriği değiştirilmiş bir e-posta ile kurbanlarına ulaşmakta ve kurbanın dikkatsizliğinden faydalanarak sistemlerine sızmaktadırlar. Bu saldırıda kurbanı korkutarak amaçlarına ulaşmaya çalışmışlardır.
  Son yıllarda dijital para birimi olan bitcoin, hükümetlerin denetim mekanizmasında olmadığından şüpheli alışverişlerde sıklıkla kullanılmaya başlamıştır. Bitcoin'in getirdiği bu rahatlık suçluların dikkatini çekmekte ve siber saldırılarda yaşanan büyük artışta önemli rol oynamaktadır. Fidye yazılımların ana amacı olan fidyeyi ödemek kesin çözüm olarak görülmemelidir. Fidyeyi ödemek saldırganları motive edeceğinden bu saldırıların sayısının giderek artmasına neden olacaktır. Saldırılar hazırlanırken şifrelenen dosyaların erişiminin engellenmesini sağlamak amacıyla her kullanıcıya farklı bir şifre anahtar üretilmektedir. Genellikle bu şifreler bir alanda tutulmamakta, kurban fidyeyi ödediği takdirde rastgele bir şifre anahtarı gönderilmekte ve kurban dosyalarına erişim sağlayamamaktadır. Bazı saldırılarda da fidye ödense bile hiçbir şekilde yanıt verilmemektedir. Bu ve benzeri nedenlerle fidye ödemek çözüm olarak görülmemektedir.

Son yıllarda yaşanan saldırılar ve verdiği zararlar düşünüldüğünde siber suçlarla başa çıkmak için basit önlemler yerine daha fazlasına ihtiyaç duyulduğu açıktır. En kötü senaryo durumu düşünülerek saldırıya uğramadan gerekli önlemler alınması gereklidir. Bu önlemler genel olarak:

- Kaynağı bilinmeyen şüpheli e-postalar açılmamalı, güvenli olmayan internet siteleri ziyaret edilmemelidir.
- Kullanılan programların güncel olması sistemde güvenlik zafiyeti oluşmasını önlemektedir.

• Güvenli ve güncel bir anti virüs ya da sandbox uygulamasını kullanmak çoğu saldırıyı engellemeye yardımcı olmaktadır.
• Kullanıcıların, değerli dosyalarını farklı bir sistemde düzenli olarak yedeklemesi; olası bir saldırıda alternatif olarak saldırı öncesi anına dönülmesinde önemlidir.
• Kullanıcıların karşı karşıya bulundukları tehlikeler hakkında farkındalık yaratılması ve alınması gereken önlemleri hakkında bilgilerinin olması gereklidir.

Bu çalışma; fidye yazılımlar ve teknik analiz içermesi nedeniyle önemlidir. Araştırmanın yalnızca siber güvenlik uzmanları üzerinde değil, yapılacak benzer araştırmalarda ve kişisel kullanıcılar ve kurumlara üzerinde de olumlu bir etki yaratması beklenmektedir.

5. KAYNAKLAR (REFERENCES)

[1] Yılmaz, E. N., Gönen, S., & Ulus, H. İ. (2016). Bilişim alanında işlenen suçlar üzerine bir inceleme. Bilişim Teknolojileri Dergisi, 9(3), 229.

[2] Çetin, H., Gundak, İ., & Çetin, H. H. (2015). E-işletme güvenliği ve siber saldırılar üzerine bir araştırma. Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 6(2), 223-240.

[4] İlker, Kara. Teslacrypt fidye yazılım virüsünün tespiti, teknik analizi ve çözümü. Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 2(2), 87-94.

[3] Kara, I., & Aydos, M. (2018, December). Static and Dynamic Analysis of Third Generation Cerber Ransomware. In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 12-17). IEEE.

[5] Öğün, M. N., & Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. Security Strategies Journal, 9(18).

[6] Yiğit, T., & Akyıldız, M. (2014). Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 18(1), 14-21.

[7] İlker, Kara. (2015). Türkiye de zararlı yazılımlarla mücadelenin uygulama ve hukuki boyutunun değerlendirilmesi. Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi, (52), 87-98.

[8] Kara, İ., & Aydos, M. (2019). The ghost in the system: technical analysıs of remote access trojan. International Journal on Information Technologies & Security, 11(1).

[9] Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2018). Ransomware payments in the bitcoin ecosystem. arXiv preprint arXiv:1804.04080.

[10] Zavarsky, P., & Lindskog, D. (2016). Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. Procedia Computer Science, 94, 465-472.

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

[12] Dhawan, S., & Narwal, B. (2019). Unfolding the Mystery of Ransomware. In International Conference on Innovative Computing and Communications (pp. 25-32). Springer, Singapore.

[13] Zimba, A., & Chishimba, M. (2019). On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. European Journal for Security Research, 1-29.

[14] Yan, S. Y. (2019). Offensive Cryptography. In Cybercryptography: Applicable Cryptography for Cyberspace Security (pp. 413-429). Springer, Cham.

[15] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015, July). Cutting the gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 3-24). Springer, Cham.

[16] Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., ... & McCoy, D. (2018, May). Tracking ransomware end-to-end. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 618-631). IEEE.

[17] O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. IET Networks, 7(5), 321-327.

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

[19] Chadha, S., & Kumar, U. (2017, May). Ransomware: Let's fight back!. In 2017 International Conference on Computing, Communication and Automation (ICCCA) (pp. 925-930). IEEE.

[20] Ahn, G. J., Doupe, A., Zhao, Z., & Liao, K. (2016). Ransomware and cryptocurrency: partners in crime. In Cybercrime Through an Interdisciplinary Lens (pp. 119-140). Routledge.