Açık Anahtar Altyapısı ile Dijital İmzalamanın Zararlı Yazılımlar Üzerindeki Etkisi

***

Impact of Digital Signing on Malware in Public Key Infrastructure

Mehmetcan TOPAL[1]
Zeynep ALTAN[2]

DOI:10.33461/uybisbbd.1507316

Makale Bilgileri

Makale Türü: Araştırma Makalesi

Geliş Tarihi: 29.06.2024

Kabul Tarihi: 19.08.2024

Öz

Geçmişten günümüze şifreleme, pek çok uygulamada kullanılan farklı yöntemleriyle büyük bir evrim geçirmiştir. Güçlü şifreleme algoritmalarının zaman içerisindeki gelişimi, dijital iletişimde güvenliği sağlayan Açık Anahtar Altyapısını oluşturmuştur. Bu altyapının önemli bir bileşeni olan dijital imzalama günümüzde yaygın olarak kullanılmaktadır ve verinin doğruluğunu, bütünlüğünü ve güvenilirliğini önemli ölçüde sağlamaktadır. Bu çalışmada dijital imzalama yöntemlerinin, günümüz siber güvenlik dünyasında, zararlı yazılımların güvenilirliği üzerindeki etkisi değerlendirilmektedir. Zararlı yazılımların etkileri ve sonuçları her geçen gün artmakta olup, yaygın olarak kullanılan e-imza ve dijital sertifikalar da bu etkileri artırabilmektedir. Bu bağlamda çalışma, farklı yöntemlerle oluşturulan örneklere dijital imzalama uygulanarak, zararlı yazılımların güvenilirlik ölçütlerinin karşılaştırmasını içermektedir. Testler sonucunda imzalı olan zararlı uygulamaların imzasız olan zararlı uygulamalara göre daha düşük olasılıkla güvenlik sistemlerine yakalandıkları ölçülmüştür. Özetle araştırma, dijital imzalamanın zararlı yazılımların yayılımını ne ölçüde etkilediğini ortaya koymayı ve siber güvenlik önlemlerinin geliştirilmesine katkı sağlamayı amaçlamaktadır.

Anahtar Kelimeler: *Açık Anahtar Altyapısı, Dijital İmza, Şifreleme, Zararlı Yazılım.*

Article Info

Paper Type: Research Paper

Received: 29.06.2024

Accepted: 19.08.2024

Abstract

From past to present, cryptography has undergone a significant evolution from past to present, with various methods used in many applications. The development of strong encryption algorithms over time has established the Public Key Infrastructure, which ensures security in digital communication. A key component of this infrastructure, digital signing, is widely used today and plays a crucial role in ensuring the accuracy, integrity, and reliability of data. This study evaluates the impact of digital signing methods on the reliability of malware in the context of today's cybersecurity landscape. The effects and consequences of malware are increasing day by day, and commonly used e-signatures and digital certificates may also exacerbate these impacts. In this context, the study includes a comparison of the reliability metrics of malware by applying digital signing to examples created using different methods. Tests have shown that signed malware applications are less likely to be detected by security systems compared to unsigned ones. In summary, this research aims to reveal the extent to which digital signing affects the spread of malware and to contribute to the development of cybersecurity measures.

Keywords: *Public Key Infrastructure, Digital Signature, Cryptography, Malware.*

Atıf/ to Cite (APA): Topal, M. & Altan Z. (2024). Açık Anahtar Altyapısı ile Dijital İmzalamanın Zararlı Yazılımlar Üzerindeki Etkisi. Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 8(2), 99-109. DOI: 10.33461/uybisbbd.1507316

[1] Beykent Üniversitesi, Mühendislik-Mimarlık Fakültesi, mehmetcantopal9@hotmail, İstanbul, Türkiye.
[2] Dr. Öğr. Üyesi, Beykent Üniversitesi, Mühendislik-Mimarlık Fakültesi, zeynepaltan@beykent.edu.tr, İstanbul, Türkiye.

1. GİRİŞ

Açık anahtar altyapısının dijital iletişimde güvenliği sağlamadaki rolü bilişim dünyasında etkindir. Açık anahtar altyapısının temel özelliği, veri transferi sırasında farklı şifreleme yöntemleriyle gizliliği sağlamadaki kritik önemidir. Güçlü şifreleme yöntemleri ve dijital imzalama teknikleri, kullanıcıların verilerini korurken aynı zamanda kimlik doğrulaması da sağlarlar (Stallings, 2017). Açık anahtar altyapısının çevrimiçi alışveriş, bankacılık işlemleri, e-posta güvenliği ya da kimlik doğrulama gibi farklı uygulama alanlarında kullanılması, kullanıcı verilerini çeşitlendirmektedir. Bu çeşitlilik doğrultusunda verilerin korunmasındaki önem ve öncelik de artmaktadır. Bu bağlamda, açık anahtar altyapısının dijital imzalama ile bağlantısı da önemli olmaktadır. Dijital imzalama, herhangi bir belgenin veya iletişimin kimlik doğruluğunu, bütünlüğünü ve orijinalliğini sağlamada kullanılmaktadır (Garfinkel & Spafford, 2002). Böylece farklı tipteki verinin korunması ve güvenilirliği sağlanarak zararlı yazılımlar tespit edilebilir ve önlenebilir.

Açık anahtar altyapısı ve dijital imzalamanın zararlı yazılımlar üzerindeki etkileri incelendiğinde, bu teknolojilerin siber güvenlikte ne kadar kritik oldukları görülür. Açık anahtar altyapısı dijital imzalama ile verileri bütünleştirir; kimlik doğrulaması yaparak güvenli iletişimi destekler. Buna rağmen, özel anahtarın kötü niyetli saldırganların eline geçmesiyle güvenlik önlemleri zararlı yazılıma dönüşmekte, dosyanın güvenli bir şekilde imzalandığı ve güvenilir bir kaynaktan geldiği izlenimi yaratılmaktadır (Mike & Davis, 2021). Bu nedenle alınan güvenlik yöntemleri araştırılmalı, mevcut yöntemlerle nasıl birleştirilebileceği ve siber tehditlerin sürekli değişen yapısına nasıl uyarlanabileceği bilinmelidir.

Siber saldırıların yaygınlaşmasıyla birlikte, açık anahtar altyapısı ve dijital imzalama teknolojileri, siber güvenlik uzmanlarının ve kuruluşların verilerini korumada ve siber saldırılara karşı dirençli olmalarında önemlidir. Bunlar, sürekli olarak geliştirilen ve mevcut yöntemlerin iyileştirildiği dinamik alanlardır. Açık anahtar altyapısındaki zararlı yazılımların kötüye kullanılması ve bu bağlamda ortaya çıkan güvenlik açıklarının etkileri giderek artmaktadır. Bu çalışma, bu sorunu derinlemesine incelemek, açık anahtar altyapısının güvenliğini artırmak ve zararlı yazılımların tespit edilmesi için etkili çözümler sunmayı amaçlamaktadır. Böylece bilgi güvenliği alanındaki diğer araştırmalar için de bir ön çalışma niteliği taşımaktadır. Çalışmada özetle, karşı bağlantı sağlamaya yarayan farklı zararlı yazılımlar üzerinden güvenlik sistemlerine yakalanma durumları araştırılmaktadır. Dijital imzalama, ilk olarak netcat[3] .exe adlı araca ve kullanımı açık olan msfvenom[4] adlı aracın zararlı işlemini şifreleme uygulanarak gerçekleştirilmiştir. Yapılan testler sonunda imzalı zararlı uygulamaların imzasız zararlı uygulamalara göre güvenlik sistemleri tarafından yakalanma olasılıklarının daha düşük olduğu sonucu çıkarılmıştır.

1.1 Geçmişten Günümüze Önemli Siber Saldırılar

Siber saldırılar, dijital çağın en büyük tehditlerinden biri olarak ortaya çıkmıştır. Bu tür saldırılar, bilgi güvenliğini tehlikeye atarak bireyler ve kurumlar için ciddi riskler oluşturur. Tarihsel olarak, çeşitli siber saldırılar bilgisayar sistemlerini ve ağlarını hedef almış, güvenlik açıklarından yararlanarak veri çalmış veya sistemleri işlemez hale getirmiştir.

Tablo1'de uluslararası ölçekte büyük etki yaratan siber saldırılar verilmekte ve bunlarla ilgili açıklamalar yapılmaktadır. Her bir saldırı ait olduğu sektörü farklı şekilde etkilemiştir.

[3] Netcat, TCP ve UDP protokollerini kullanarak ağ bağlantıları üzerinde veri okuma ve yazma işlemleri gerçekleştiren bir komut satırı aracıdır.
[4] Msfvenom, Metasploit Framework'ün bir parçası olan ve zararlı yazılım oluşturmak, çeşitli kod yüklerini ve kod çeviricilerini birleştirmek için kullanılan bir komut satırı aracıdır.

Tablo 1: Tarihteki Önemli Siber Saldırılar

İsim	Açıklama	Kaynak
Morris Solucanı (1988)	İnternet'in erken dönemlerinde dünya ölçeğinde bilgisayar ağlarını etkileyen ilk büyük saldırıdır. Bilgisayar sistemlerindeki güvenlik açıklarından yayılmıştır.	Spafford, 1988
Sony Pictures Siber Saldırısı (2014)	Şirketlerin güvenlik önlemlerini güçlendirmesi gerektiğine ilişkin bir uyarı niteliğindeydi ve siber saldırıların işletmelerin itibarlarına olası zararlarını yansıtmaktaydı.	Peterson, 2014
Stuxnet Saldırısı (2010)	İran'ın nükleer programını hedef alarak engellemeye çalışan ve devletler arasında bir siber savaş başlatabilecek güçteki karmaşık bir siber saldırıdır.	Zetter, 2014
WannaCry (2017)	Büyük ölçekli bir fidye yazılımı saldırısıdır; EternalBlue isimli bir güvenlik açığından yararlanarak bilgisayar sistemlerini kilitlemiş ve kuruluşlardan fidye talep etmiştir.	Greenberg, 2017
Moonlight Maze (1996-1998)	Amerikan savunma ve istihbarat ağlarına erişmiştir. Döneminin en karmaşık ve etkili siber casusluk saldırısıdır.	Haizler, 2017
Melissa Virüsü (1999)	e-posta kullanıcılarını etkilemiştir. Bilgisayar sistemlerinde önemli veri kayıplarına ve performans sorunlarına yol açmıştır. e-posta güvenliğinde ciddi farkındalıklara neden olmuştur.	Taylor, 2020
NotPetya saldırısı (2016)	Fidye yazılımı olarak başlamış, daha sonra bir siber sabotaj olayına dönüşmüştür. Başlangıçta Ukrayna'daki kuruluşları hedef alan bu saldırı, dünya ölçeğinde pek çok bilgisayarı etkilemiş ve büyük krize neden olmuştur.	(Fayi, 2018)
Colonial Pipeline Saldırısı (2021)	DarkSide fidye yazılımı ile etkisi altına aldığı tüm operasyonları kilitlemiştir. Bu saldırı, enerji sektöründe siber güvenlik risklerine ilişkin endişeleri arttırmıştır.	Robertson & Turton, 2021) .
Emotet Saldırısı	Bilgisayar ağlarına sızarak kötü amaçlı e-postalar gönderen ise botnet ağıdır. Bankaların bilgilerini çalan, fidye yazılımlar indiren ve pek çok zararlı eylemde bulunmuş ve pek çok kuruluş için ciddi güvenlik riski oluşturmuştur.	Europol, 2021
AnyDesk Saldırısı (2024)	Bilgisayar korsanlarının Aralık 2023 sonlarında sistemlere girdiği bir operasyondur. Saldırganlar, kritik kişisel bilgileri ve bazı şirkete ait belgeleri ele geçirmişlerdir.	Sporx, 2024

Saldırılarda kullanılan dosyalar üzerinde güvenlik önlemleri alınmasına rağmen, sızdıkları sistemlerde görünmeden hareket etmeleri sonucunda zararlı yazılımların tümü hedefine ulaşmıştır. Bunun nedeni, şaşırtma, morfizm, şifreleme, enjeksiyon gibi yöntemlerin kullanılmış olmasıdır. Şaşırtma yöntemi, güvenlik çözümlerinin tespit edilmesi işlemini güçleştirir. Örneğin, ölü ya da önemsiz bir kod eklenmesiyle, yeniden kayıt atama ya da talimat değişikliği yapılabilir (Balakrishnan & Schulze, 2005). Morfizm, özellikle polimorfik virüsler olarak, sınırsız sayıda farklı şifre çözücü oluşturarak analizi zorlaştırmayı amaçlayan karmaşık bir tekniktir. Polimorfik virüsler, şifre çözme kodunun görünümünü kopyaladıkça değiştirmek üzere çok sayıda gizleme tekniği kullanır (Rad ve diğerleri, 2012). Şifreleme, zararlı uygulamanın ikili sistemde şifrelenmesidir; uygulamanın çalışabilmesi için çalışmadan önce tekrar deşifre edilerek yüklenmesi gerekir (Tasiopoulos & Katsikas, 2014). DLL dosyaları çift tıklama ile doğrudan çalışmadığı için, DLL formatındaki kötü amaçlı bir kod derlendiğinde doğrudan çalışmayacaktır. Bu dosyanın çalışması için explorer.exe gibi bir platformda ana bilgisayar tarafından yükleniyor gibi çalıştırılması gerekir; böylece zararlı

uygulama saldırgan tarafından gizlenir (Monnappa, 2018). Bir başka zararlı uygulama olan işlem enjeksiyonu, kötü amaçlı bir işlemi başka bir işlemin bellek alanında çalıştırarak uygulamayı gizlemek amacıyla kullanılan bir yöntemdir. Enjekte edilen işlem, ana bilgisayarın yetkilerini ele geçirir (Balaoura, 2018).

Çalışmanın sonraki bölümünde açık anahtar altyapısı ile ilgili temel tanımlamalar, karma fonksiyonları ve dijital imzalama altyapısı ile açık anahtar altyapısı güvenliği anlatımlarını içermektedir. Bölüm 3' de ise, zararlı yazılımların güvenilir sertifikalarla imzalanmasının nasıl gerçekleştirildiği örneklerle karşılaştırarak anlatılmaktadır. Sonuç Bölümünde ise, dijital imza yöntemlerinin ve güvenlik çözümlerinin kullanımının masaüstü uygulamalarının güvenilirliğini arttırmadaki etkisi özetlenmektedir.

2. AÇIK ANAHTAR YAPISI

İnternet üzerinde güvenli iletişim ve veri paylaşımının önemi günümüzde giderek artmaktadır. Açık anahtar altyapısı ise hem kimlik doğruluğunu, gizliliği, veri bütünlüğünü sağlamada kritik bir rol oynamakta hem de dijital sertifikaların, dijital imzaların ve şifreleme anahtarlarının güvenilir dağıtımını ve yönetimini sağlamaktadır. Açık anahtar altyapısının çalışma ilkesi temel olarak her kullanıcının açık ve özel anahtar şeklinde bir çift anahtara sahip olmasıdır. Açık anahtar genel olarak erişilebilir ve diğer kullanıcılarla paylaşılabilir. Özel anahtar ise sadece kullanıcısına özeldir ve gizli tutulmalıdır. Bu anahtar çiftleri, açık anahtar altyapısının güvenli iletişimi sağlamadaki çatısını oluşturur.

Açık anahtar altyapısı ve dijital imzalamada verilerin doğruluğu için karma fonksiyonları önemli yer tutar. Karma fonksiyonları, verilerin benzersiz bir diziye dönüştürülmesini sağlarlar. Ayrıca veriyi sabit boyutlu bir çıktıya dönüştüren matematiksel işlevlerdir. Bu işlevler, girdinin boyutu ne olursa olsun, genellikle sabit bir boyutta bir çıktı üretir. Karma fonksiyonları genellikle bir dizi rastgele karakterden oluşur ve girdinin herhangi bir değişikliğinde bile farklı bir değer üretilir. Öncelikle, dosyanın veya veri bloğunun karma değeri hesaplanır. Daha sonra, veri veya dosyanın değiştirilmediğinden emin olmak için bu değer yeniden hesaplanır. İki karma değeri eşleşirse, verinin değiştirilmediği doğrulanır. İki karma değeri eşleşmiyor ise veri değiştirilmiştir (Paar & Pelzl, 2010).

Dijital imzalama, bir belgenin veya iletişimin doğruluğunu, bütünlüğünü ve orijinalliğini doğrulamada kullanılır. Bu süreçte, belgeyi imzalayan kişinin kimliği doğrulanır ve belgenin imzalı olduğu ve değiştirilmediği garanti altına alınır. Dijital imzalama genellikle internet üzerindeki güvenli bağlantılarda, e-postalarda veya şifrelemelerde kullanılır. Dijital sertifika ile internet ortamında kimlik doğrulanmış olur; bir belge imzalandığında, imzalayan taraf belgenin içeriğini bilmekle birlikte kendisine ait olduğunun onayını vermiş ve kendisi tarafından yollandığını belirtmiş olur (Nash ve diğerleri, 2001).

Dijital imzalama işlemi, genellikle üç temel adımdan oluşur: karma değeri hesaplama, şifreleme ve doğrulama. İlk adımda, belgenin karma değeri hesaplanır. Bu, belgenin bütünlüğünü ve orijinalliğini doğrulamak için kullanılır. İkinci adımda, belgenin karma değeri simetrik veya asimetrik şifreleme yöntemlerinden biriyle şifrelenir. Simetrik şifrelemede, verinin şifrelenmesi ve çözülmesi için aynı anahtar kullanılır. Bu yöntem hızlıdır ve verimli bir şekilde işlem yapar, ancak anahtarın güvenliğini sağlamak kritik öneme sahiptir. Asimetrik şifrelemede ise, verinin şifrelenmesi ve çözülmesi için iki farklı anahtar kullanılır: biri açık anahtar ve diğeri özel anahtar. Bu yöntem, anahtarların güvenliğini sağlasa da işlem süreci daha karmaşıktır. Üçüncü adımda, alıcı, belgenin karma değerini ve imza olarak alınan şifrelenmiş karma değerini açık anahtarıyla çözer ve bu iki değeri karşılaştırır. Eşleşme durumunda, belgeyi imzalayan kişi ve belgenin bütünlüğü doğrulanmış olur. İki değerin eşleşmemesi durumunda verinin değiştirildiği kabul edilir ve alıcı taraf bu durum ile ilgili olarak bilgilendirilir.

Özellikle çevrimiçi işlemler ve iletişimlerde, dijital imzalama ve karma fonksiyonları, verilerin güvenliğini sağlamada temel önlemler olarak kabul edilmektedir.

2.1. Açık Anahtar Altyapısı Güvenliği

Açık anahtar altyapısı, dijital iletişimde güvenliği sağlamak için yaygın olarak kullanılan bir sistemdir. Dijital sertifikalar, dijital imzalar ve şifreleme anahtarlarının güvenilir dağıtımı ve yönetimini sağlamasına rağmen, açık anahtar altyapısının bazı zayıf noktaları vardır. İlki, güvenilirlik ve kimlik doğrulama sorunudur. Açık anahtar altyapısı, genellikle bir üçüncü tarafın güvenilirliğini gerektirir. Ama bu garanti değildir ve saldırganlar tarafından hedef alınabilirler. Böylece, sertifika yetkilileri veya sertifika dağıtımı ile açık anahtar altyapısı bileşenlerinin güvenliği zayıflar. Bir başka zayıf nokta da anahtar yönetimidir. Anahtarların güvenliği sağlanmadığında, şifreleme anahtarlarının ele geçirilmesi veya kötü niyetli kullanımı gibi riskler ortaya çıkabilir. Anahtar yönetimi, dikkatli bir şekilde yapılmalı ve anahtarların güvenliği için sıkı güvenlik önlemleri alınmalıdır. Diğer taraftan, yanlış algoritmaların veya zayıf parametrelerin kullanılması da kriptografik güvenliği tehlikeye atabilir. Güvenilmeyen ve zayıf kimlik doğrulama süreçleri çok faktörlü kimlik doğrulamalarla sağlamlaştırılmalıdır. Saldırganlar, sosyal mühendislik taktikleri ile sisteme sızabilirler ve kullanıcıları manipüle ederek kimlik bilgilerini ele geçirebilirler (Klimburg-Witjes&Wentland, 2021). Hatta fiziksel erişim ile anahtarları veya cihazları çalabilirler İnsan faktörü de açık anahtar altyapısını etkileyebilir. Güçlü şifrelerin kullanılmaması, anahtarların korunmasında dikkatsizlik, güvenli olmayan ağlarda iletişim, güncellenmemiş yazılımlar gibi pek çok etken, insan hatalarından kaynaklı olarak açık anahtar altyapısının güvenliğini tehlikeye sokmaktadır.

3. ZARARLI YAZILIMLARIN GÜVENİLİR SERTİFİKALARLA İMZALANMASI

Zararlı yazılımların güvenilir sertifikalarla imzalanması, yazılımın güvenli olduğu anlamına gelmez. Aksine, bu tür yazılımlar kötüye kullanılarak kullanıcıları ve sistem yöneticilerini yanıltabilir ve güvenlik riski doğurabilir. Buna rağmen, güvenilir sertifikalarla imzalanmış yazılımlar, kişiler ve güvenlik yazılımları tarafından daha güvenilir kabul edilir. Böylece kullanıcılar ve sistem yöneticileri yanıltılarak güvenlik yazılımları atlatılabilir. Zararlı yazılım geliştiricileri, sahte veya çalıntı sertifikalar kullanarak yazılımlarını imzalayabilirler. Bu nedenle, güvenilir sertifikaya sahip bir yazılım bile kötü amaçlı olabilir. Diğer bir ifade ile, zararlı bir yazılım güvenilir sertifikalarla imzalanarak güvenlik önlemlerini atlatarak sisteme sızabilir. Bu durumda sistem, veri kaybı, kimlik hırsızlığı, finansal kayıp ve daha birçok soruna açık hale gelir.

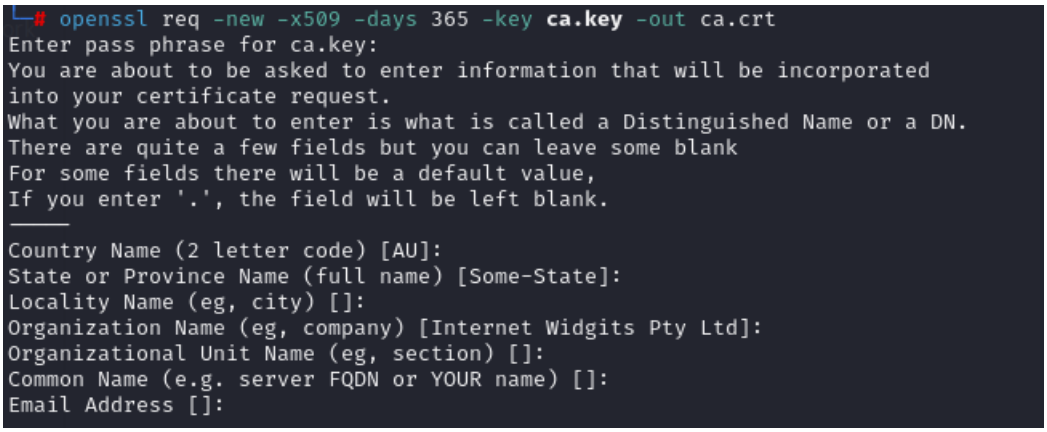
Zararlı yazılımların güvenilir sertifikalarla imzalanarak güvenilirlik sağlama girişimi büyük bir risktir. Güvenilir sertifikalar, genellikle güvenilir olduğu düşünülen ve sertifika yetkilileri tarafından onaylanan kuruluşlar tarafından sağlanır. Ancak, kötü niyetli aktörler bu sertifikaları kötüye kullanarak zararlı yazılımları imzalamak ve yaymak için güvenilirlik algısını suistimal edebilirler.

3.1. Zararlı Yazılım Uygulaması

Bu bölümde, ilk olarak nc.exe uygulaması ve şifreleme uygulanmış msfvenom aracı ile oluşturulan kötü amaçlı yük kullanılarak, dijital imza yöntemiyle zararlı yazılımların güvenilirlik algısının arttırmasına yönelik bir uygulama yapılmaktadır. Genellikle sızma testleri ve güvenlik açığı uygulamalarıyla kötü amaçlı zararlı yazılımlar oluşturularak hedef sistemlere saldırı gerçekleştirilir. Bu yazılımlar hem farklı işletim sistemleri ve platformlar tarafından desteklenir, hem de dosyanın bazı özellikleri özelleştirilerek farklı modüllerle birlikte kullanılıp etkilerini arttırılabilir. nc.exe gibi araçlar, çeşitli güvenlik açıkları ve kötü amaçlı yazılımlar için potansiyel bir kullanım alanı sağlarlar; ayrıca ağ trafiğini yönlendirme ve değiştirme yeteneklerine sahiptirler. Çalışmada nc.exe'nin karşı bağlantı sağlama özelliği kullanılmaktadır. Msfvenom aracı ile oluşturulan kötü amaçlı yükte karşı bağlantı sağlama özelliğine göre hazırlanmıştır. Böylece saldırı vektörü ve etkisi aynı, fakat yöntem ve hazırlanışı farklı olan iki uygulamanın güvenlik sistemleri üzerindeki etkisi karşılaştırılmaktadır.

Dijital imzalama için gerekli olan sertifika anahtarı OpenSSL aracı kullanılarak Şekil 1'de oluşturulmuştur (Kili, 2019). OpenSSL, çeşitli kriptografik işlemleri gerçekleştirmek için kullanılan, güvenli iletişim ve veri şifrelemesi sağlamak için yaygın olarak tercih edilen ve geniş bir topluluk desteği olan bir araçtır. Şekil 2'de ise, sertifika talebi ve özel anahtar ile X.509 standartlarına uygun sertifika görülmektedir. X.509 standardı, dijital sertifikaların oluşturulması ve yönetilmesi için yaygın olarak kullanılan bir standart olmakla birlikte kimlik doğrulama, şifreleme ve dijital imzalama gibi güvenlik işlevlerini sağlamada güvenilir bir yapı sunar. X.509, açık anahtar altyapısı içinde dünya çapında kullanılan, iyi belgelenmiş ve test edilmiş bir standarttır.

Şekil 1: Sertifika Anahtarı Oluşturma

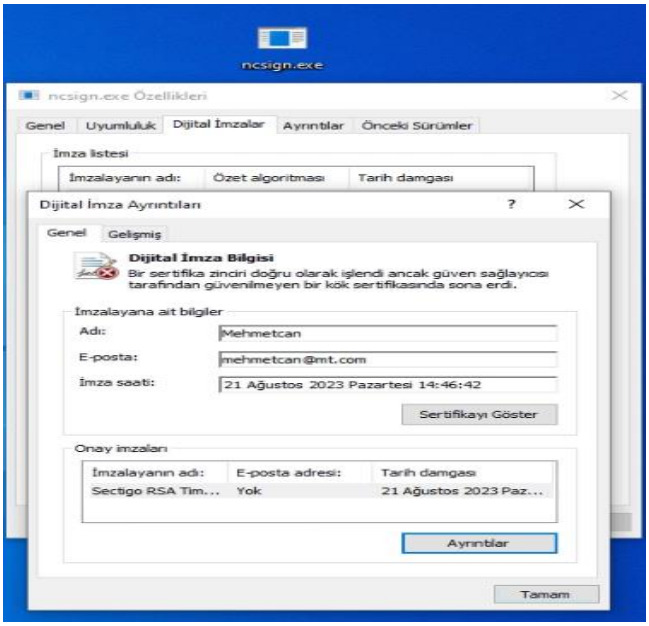


Şekil 2: Sertifika Talebi ve Sertifika Oluşturma

Şekil 3'te sertifika ve özel anahtar kullanılarak "osslsigncode" aracı ile "nc.exe" dosyasının "ncsign.exe" adı altında imzalı hâli görülmektedir.

Şekil 3: İmzalama Adımı

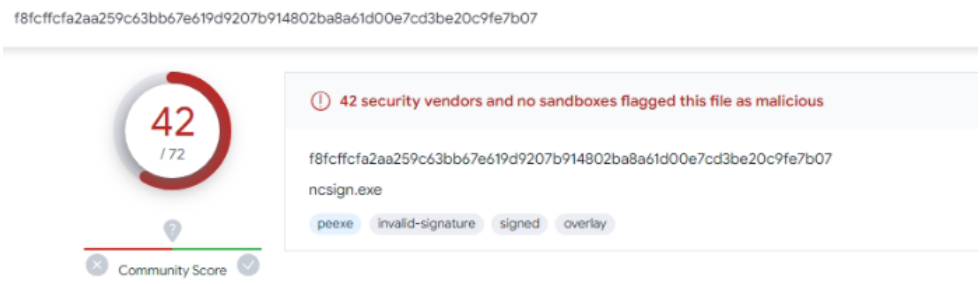
İmzalı "ncsign.exe" dosyasındaki imza bilgileri ve Şekil 1'deki sertifika talebine ait bilgiler Şekil 4'de görülebilir.



Şekil 4: İmzalama Sonrası Ayrıntılar

İmzasız olan "nc.exe" ve imzalı olan "ncsign.exe" dosyalarının, VirusTotal[5] sitesindeki antivirüs uygulamaları üzerindeki yakalanma durumları Şekil 5 ve Şekil 6'da görülmektedir. Popüler kullanımda olan antivirüs uygulamaları imzasız olan nc.exe uygulamasını zararlı olarak algılamaktadır. Doğrudan zararlı olarak algılanmasının sebebi, uygulamanın derlenmiş olarak internette yer alması, karma değerinin birçok güvenlik sisteminin veri tabanlarında zararlı olarak belirtilmesidir.

Şekil 5: "nc.exe" dosyasının VirusTotal ile kontrolü



Şekil 6: "ncsign.exe" dosyasının VirusTotal ile kontrolü

[5] Kötü amaçlı yazılımlar ve diğer ihlallerin tespiti için şüpheli dosyaların, etki alanlarının, IP'lerin ve URL'lerni analiz edildiği ve bunların otomatik olarak paylaşıldığı platform.

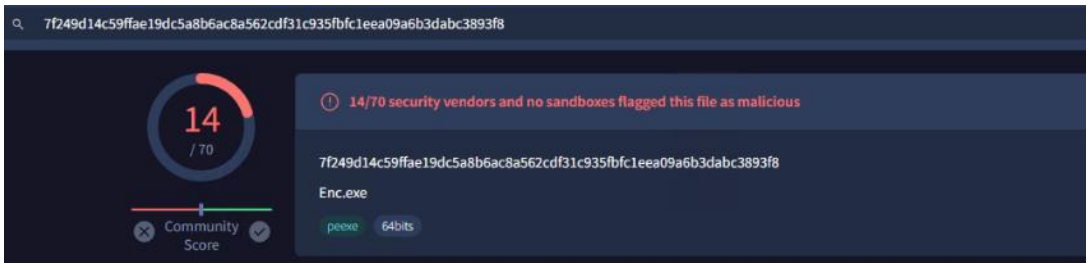
Şekil 7'de "nc.exe" uygulamasının karşı bağlantı sağlama özelliği ile aynı işleve sahip farklı bir uygulama incelenmektedir. Msfvenom aracı ile karşı bağlantı sağlayan kötü amaçlı yük değeri alınmıştır. Bu değer ilk olarak önceden bir XOR işlemine girmiştir. Böylece başlangıçtaki şifreli değer anlaşılmayacak hale getirilmiştir.

```
unsigned char encrypted_shellcode[] = {
    "0xbd, 0x9, 0xc2, 0xa5, 0xb1, 0xa9, 0x8d, 0x41, 0x41, 0x41, 0x0, 0x10, 0x0, 0x11, 0x13, 0x10, 0x17, 0x9, 0x70, 0x93,
};

// Decrypt function
void decryptShellcode(unsigned char* shellcode, size_t size) {
    for (int i = 0; i < size; ++i) {
        shellcode[i] ^= XOR_KEY;
    }
}

int main() {
    // Decrypt the shellcode
    decryptShellcode(encrypted_shellcode, sizeof(encrypted_shellcode));

    // Allocate memory for the shellcode
    void* mem = VirtualAlloc(0, sizeof(encrypted_shellcode), MEM_COMMIT, PAGE_EXECUTE_READWRITE);
    if (mem == NULL) {
        std::cerr << "Failed to allocate memory!" << std::endl;
        return 1;
    }

    memcpy(mem, encrypted_shellcode, sizeof(encrypted_shellcode));
```

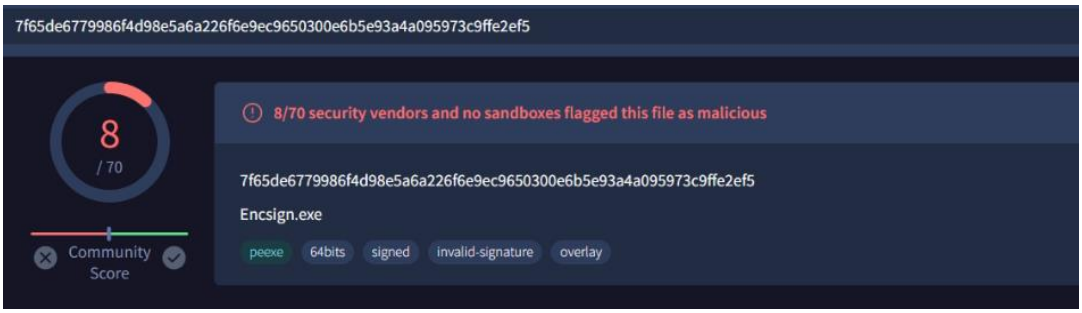
Şekil 7: Özel Uygulamaya ait Kaynak Kod

XOR, basit bir şifreleme formudur ve genellikle verileri gizlemek için kullanılır. Temelinde simetrik şifrelemeye dayanır. Uygulama çalıştırıldığında, XOR işlemi ile şifrelenmiş veri deşifre edilerek çözümlenme işleminde byte değerleri tek tek belleğe yazılmakta ve tekrardan çalışır duruma getirilmektedir.

Burada uygulamanın "Enc.exe" olarak derlenmesinden sonra, Şekil 3'teki gibi imzalama adımı uygulanmış ve "Encsign.exe" adlı dosya oluşturulmuştur. "Enc.exe" ve "Encsign.exe" uygulamalarının VirusTotal üzerindeki yakalanma durumları Şekil 8 ve Şekil 9'da yer almaktadır.



Şekil 8: VirusTotal'de Enc.exe



Şekil 9: VirusTotal'de Encsign.exe

Sonuç olarak, bu çalışmada aynı işleve sahip farklı zararlı uygulamaların güvenlik sistemlerine yakalanma durumları incelenmiştir. Gerçekleştirilen testler doğrultusunda imzalı olan zararlı uygulamaların imzasız olan zararlı uygulamalara göre güvenlik sistemleri tarafından yakalanma olasılığının daha düşük olduğu gözlemlenmiştir (Tablo 2). Buradan da dijital imzalamanın, güvenilirlik ölçütünün artmasında etkili olduğu sonucu çıkarılabilir.

Tablo 2: Uygulamaların Karşılaştırılması

	İmza Durumu	**Başarı Oranı**
nc.exe	İmzasız	51/70
ncsign.exe	İmzalı	42/72
Enc.exe	İmzasız	14/70
Encsgin.exe	İmzalı	8/70

5. TARTIŞMA VE SONUÇ

Bu çalışmada, dijital imzalama yöntemi ile zararlı uygulamaların güvenilirlik etkileri, açık anahtar altyapısı kapsamında incelenmiştir. Dijital imza, dosyaların veya uygulamaların orijinal ve güvenilir kaynaklardan geldiğini doğrulamak için kullanılan önemli bir araçtır. Bu bağlamda zararlı uygulamaların güvenilirlik seviyelerini artırmak amacıyla dijital imza yöntemlerinin uygulamalara olan etkilerine odaklanılmıştır.

Sonuçların imzalamadan dolayı mı ya da ilgili dosyaların karma değerinin değiştiğinden dolayı mı farklılık gösterdiği bu çalışma doğrultusunda cevaplanması gereken önemli bir sorudur. Karma değerinin kaynak kod üzerindeki bir değişiklikten dolayı değişmesi de VirusTotal gibi sitelerdeki etkisini elbette değiştirebilmektedir. Bu durumla ilgili bir çalışma olarak canlı ortamlarda farklı güvenlik sistemleri üzerinde çalışmalar yapılmıştır. Fakat, etik olarak isim ve ekran görüntüsü paylaşılmamaktadır. Yapılan uygulamalarda kaynak kodu aynı olan zararlı uygulama farklı zamanlarda derlenerek farklı karma değerli halleri üretilmiştir. İki uygulamanın da canlı ortamda güvenlik sistemlerine yakalandığı tespit edilmiştir. Bu iki uygulamanın dijital imzalama sonucu aynı güvenlik sistemleri üzerinde başarılı sonuçlar verdiği görülmüştür. VirüsTotal üzerinde de başarı oranının arttığı görülmektedir. İlgili güvenlik sistemlerinin yapılandırmaları bu çalışma için elbette büyük önem taşımakta ve fark yaratmaktadır.

Güvenlik önlemlerini aşmanın farklı yolları vardır. Bunlar kod betikleri, şifreleme teknikleri, özel olarak oluşturulmuş kütüphaneler ve güvenlik ürünlerinin çalışma mantığına göre değişir. Günümüzde internet güvenliği için birçok araştırma ve çalışma yapılmaktadır. e-Ticarette kredi kartı bilgilerinin korunması, güvenli iletişim sağlanması gibi konularda yoğun çalışmalar devam etmektedir. Siber saldırılar, bireylerden veya kuruluşlardan gelebilir. Bunlar genellikle güvenlik ölçütlerinin etkinliği ile yakından ilişkilidir. Bu bağlamda, çalışmanın odağında açık anahtar altyapısında önemli bir rol oynayan dijital imzalama tekniğinin zararlı yazılımlar üzerindeki etkileri ve güvenlik ürünlerinin tepkileri olmuştur. Dijital imza tekniği, sadece güvenlik ürünlerini atlatmak için değil, aynı zamanda kullanıcıları da aldatmak için de kullanılabilir. Kullanıcılar, bir uygulama indirildiğinde sertifikasız olduğunda uyarılır ve kullanıcı genellikle bu uyarıyı kapatır. Ancak, sertifikalı bir uygulama indirildiğinde, sistem tarafından güvenli olarak kabul edildiğinden, kullanıcılar genellikle uygulamayı güvenli kabul edip çalıştırır. Bu durum, kullanıcıları yanıltmak için çeşitli dosya formatlarında kullanılabilir. Dijital olarak imzalı bir uygulamanın güvenlik çözümlerinin ve insanların güvenilirlik algısı üzerinde etkisi de fazladır. Çalışma bu faktörlerin hepsine bir uyarı niteliğindedir.

Diğer taraftan makine öğrenmesi algoritmalarıyla da zararlı yazılımların tespit edilmesi ve engellenmesi konusunda büyük ilerlemeler kaydedilmektedir. Zararlı yazılımların tespiti ve analizinde dinamik analiz tekniklerinin kullanılması, evrişimsel sinir ağları ile ikili dosya yapısına dayalı zararlı yazılım tespiti ve diğer farklı makine öğrenmesi algoritmalarının karşılaştırılması gibi yöntemlerin etkili sonuçlar verdiği görülmektedir. Bu araştırmalar, makine öğrenmesi tabanlı yaklaşımların dijital imzalama ve sertifikanın kötüye kullanımını belirlemede proaktif ve adaptif çözümler sunmaktadır. Ayrıca, zamana bağlı olarak yapılan dijital imza kontrolünün zararlı yazılımın yakalanmasına katkı sağladığına ilişkin çalışmalar da bulunmaktadır. Dijital imzaların zaman damgaları ve geçerlilik sürelerinin analiz edilmesi, zararlı yazılım tespitinde ek güvenlik sağlamaktadır. Dijital imzalama tekniği, zararlı yazılımların içerisini gizlemek için kullanılan bir yöntem olarak düşünülebilir. Makine öğrenmesi algoritmaları ile dinamik analiz sürecindeki çalışmalarla imza ve sertifika kontrollerinin geliştirilmesi, zararlı yazılımların tespit edilmesinde giderek daha fazla önem taşıyacaktır. Dinamik analizin ve yapılandırmanın iyi olduğu sistemlerde dijital imzalamanın, güvenlik ürünlerini atlatma adımlarında bir etkisi olmadığı da görülmektedir. Gelecekte, bu tekniklerin daha da geliştirilmesi ve geniş çapta uygulanmasıyla, zararlı yazılımlara karşı daha yüksek düzeyde koruma sağlanabilecektir.

KAYNAKÇA

Balakrishnan, A. & Schulze, C. (2005). Code Obfuscation Literature Survey. Computer Sciences Department, University of Wisconsin.

Balaoura, S. (2018). Process Injection Techniques and Detection Using the Volatility Framework. Master's thesis, University of Piraeus, Greece.

Europol. (2021). "World's Most Dangerous Malware EMOTET Disrupted Through Global Action". https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action

Fayi, S. (2018). What Petya/NotPetya Ransomware Is and What Its Remidiations Are. 10.1007/978-3-319-77028-4_15.

Garfinkel, S. & Spafford, E. (2002). Web Security, Privacy and Commerce. O'Reilly Media.

Greenberg, A. (2017). The WannaCry Ransomware Hackers Made Some Real Amateur Mistakes. Wired. https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/.

Haizler, O. (2017). The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking in Cyberspace, Intelligence, and Security. Vol 1. Nr.1. The Institute for Natural Security Studies. https://www.inss.org.il/wp-content/uploads/2017/03/The-United-States'-Cyber-Warfare-History-Implications-on.pdf

Kili, A. (2019). How to Generate a CSR (Certificate Signing Request) in Linux. Tecmint https://www.tecmint.com/generate-csr-certificate-signing-request-in-linux

Klimburg-Witjes, N. & Wentland, A. (2021). "Hacking Humans? Social Engineering and the Construction of the Deficient User in Cybersecurity Discourses", Science, Technology, & Human 46(6). 1316-1339. SAGE Journals.

Mike, C. & David, S, "Cryptography and the Public Key Infrastructure," in CompTIA Security+ Study Guide: Exam SY0-601, Wiley, 2021, pp.179-227.

Monnappa, K. A. (2018). Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware. Packt Publishing Ltd.

Nash, A., William, D. & Celia, J. (2001) PKI Implementing and Managing e-Security. McGraw-Hill.

Paar, C. & Pelzl J. (2010). Understanding Cryptography: a Textbook for Students and Practitioners. Springer.

Peterson, A. (2014). The Sony Pictures hack, explained. The Washingthon Post: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

Rad, B.B., Masrom, M. & Ibrahim, S. (2012) Camouflage in Malware: From Encryption to Metamorphism. International Journal of Computer Science Network. Security. 12 (74–83).

Robertson, J. & Turton, W. (May 8, 2021). "Colonial Hackers Stole Data Thursday Ahead of Shutdown". Bloomberg News.

Spafford, E.H. (1988). The Internet Worm Program: An Analysis. Purdue Technical Report CSD-TR-823. https://spaf.cerias.purdue.edu/tech-reps/823.pdf

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.

Sporx. (2024). AnyDesk hacklendi mi? Anydesk hack nedir? https://www.sporx.com/anydesk-hacklendi-mi-anydesk-hacked-nedir-SXHBQ1056445SXQ

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.

Tasiopoulos, V.G. & Katsikas, S.K. (2014). Bypassing Antivirus Detection with Encryption. In Proceedings of the 18th Panhellenic Conference on Informatics.

Taylor, C. (2020). Melissa Virus. CyberHoot. https://cyberhoot.com/cybrary/melissa-virus/

Zetter, K. (2014) An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Magazine Wired. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/