



Marmara Üniversitesi
Teknoloji Fakültesi Bilgisayar Mühendisliği
Bilgisayar Güvenliği Dersi Projesi

Ransomware Simülasyonu ve Savunma Mekanizmaları

Ali Mete ÇIPLAK	170422007
Mahmutcan SAKINCI	170422035
Mustafa TETİK	170422033

Arş. Gör. Barış İNCEİŞÇİ

İçindekiler

1. Giriş
2. **Literatür Taraması**
3. Ransomware'ın Tanımı ve Tarihçesi
 - 3.1. Ransomware Tanımı
 - 3.2. Ransomware Tarihçesi
4. Ransomware'ın Çalışma Prensipleri
 - 4.1. Bulaşma
 - 4.2. Yayıma
 - 4.3. Şifreleme
 - 4.4. Fidye Notu
 - 4.5. Ransomware-as-a-Service (RaaS) Modeli
5. Yaygın Saldırı Türleri ve Örnekleri
 - 5.1. Örnek Saldırıları
6. Ransomware Saldırılarının Etkileri
 - 6.1. Ekonomik Etkiler
 - 6.2. Toplumsal Etkiler
 - 6.3. Bireysel Etkiler
7. Korunma ve Müdahale Yöntemleri
 - 7.1. Altyapı Güvenliği
 - 7.2. Eğitim ve Farkındalık
 - 7.3. Yedekleme
 - 7.4. Tespit ve Müdahale
 - 7.5. Raporlama ve İşbirliği
 - 7.6. Ödeme Politikası
8. Statik Analiz
 - 8.1. Virustotal Sonuçları
 - 8.2. PESTudio ile Analiz
 - 8.3. String Analizi
9. Dinamik Analiz
 - 9.1. Analiz Ortamının Kurulumu
 - 9.2. Ağ Davranışlarının Simülasyonu
 - 9.3. Host Bazlı Davranışlar
 - 9.4. Sonuç
10. Kaynakça

1. Giriş

Günümüzde dijitalleşmenin her alanda hız kazanmasıyla birlikte siber güvenlik tehditleri de aynı ölçüde karmaşıklaşmakta ve yaygınlaşmaktadır. Bu tehditler arasında en yıkıcı etkilerden birine sahip olan fidye yazılımları (ransomware), bireylerden devlet kurumlarına kadar geniş bir yelpazede ciddi zararlar doğurmaktadır. Fidye yazılımları, hedef sistemlere sızarak kullanıcı dosyalarını şifreler ve bunların yeniden erişilebilir olması için fidye talebinde bulunur. Son yıllarda artan bu saldırılar, yalnızca ekonomik kayıplara yol açmakla kalmamış; aynı zamanda sağlık, ulaşım ve enerji gibi kritik altyapı hizmetlerinin sekteye uğramasına da neden olmuştur.

Bu çalışmada, fidye yazılımlarının işleyişi, evrimi ve yol açtığı tehditler hem teorik hem de pratik açıdan ele alınmıştır. Özellikle 2017 yılında küresel ölçekte etkili olan ve SMB protokolündeki bir güvenlik açığını kullanarak yayılım gösteren WannaCry fidye yazılımı detaylı şekilde analiz edilmiştir. Bu doğrultuda, Oracle VirtualBox ortamında oluşturulan sanal laboratuvar üzerinde WannaCry zararlısının davranışları simüle edilmiş; hem statik hem de dinamik analiz araçları kullanılarak teknik çözümler ve savunma mekanizmaları araştırılmıştır. PeStudio, Process Monitor ve Regshot gibi araçlar sayesinde fidye yazılımının sistemde yaptığı değişiklikler izlenmiş, analiz süreci boyunca elde edilen veriler yorumlanarak olası önleyici stratejiler ortaya konmuştur.

Çalışmanın temel amacı, hem güvenlik araştırmacılarına hem de bilgi güvenliği profesyonellerine, fidye yazılımlarının yapısını daha yakından tanıma ve bu tür tehditlere karşı alınabilecek önlemler konusunda farkındalık kazandırmaktır. Ayrıca, theZoo gibi açık kaynaklı zararlı yazılım arşivlerinin eğitim ve araştırma amaçlı kullanımı ile gerçek zararlılar üzerinde kontrollü analiz yapmanın önemi vurgulanmaktadır.

2. Literatür Taraması

Hsiao ve Kao tarafından gerçekleştirilen bu çalışmada[1], WannaCry fidye yazılımı örneği üzerine kapsamlı bir statik analiz yapılmıştır. Yazarlar, tersine mühendislik yaklaşımıyla WannaCry'nin çok aşamalı çalışma yapısını detaylandırmış; dağıtım, kurulum, şifreleme ve komuta-kontrol (C&C) olacak şekilde dört ana fazı incelemiştir. Analiz sürecinde, IDA Pro adlı disassembler aracı kullanılarak WannaCry'nin bileşenleri ayrıştırılmış ve her birinin sistemdeki işlevi açıklanmıştır. EternalBlue güvenlik açığı ve DoublePulsar arka kapısı kullanılarak sistemlere nasıl sızıldığı; bellek içi çalışan launcher.dll'in mssecsvc.exe adlı bileşeni oluşturmak için nasıl kullanıldığı; ardından tasksche.exe aracılığıyla zararlı yüklerin sistemde nasıl yapılandırıldığı ayrıntılı biçimde ortaya konmuş. Şifreleme aşamasında RSA-2048 ve AES-128 algoritmalarının birlikte kullanıldığı ve her dosya için benzersiz anahtarlar üretildiği, bu anahtarların da saldırganın sahip olduğu kök anahtarla şifrelendiği belirtilmiştir. Komuta-kontrol aşamasında ise TOR ağı üzerinden iletişim kurularak fidye ödeme süreçlerinin takip edildiği ve sistem bilgileri toplandığı vurgulanmıştır. Çalışma, WannaCry'nin bileşenlerinin büyük ölçüde modüler ve yeniden kullanılabilir şekilde tasarlandığını göstermektedir.

Yine aynı yazarların WannaCry'nin dinamik analizini yaptıkları bu çalışma[2], fidye yazılımının sisteme bulaştıktan sonraki tüm etkileşimlerini süreçler, dosya sistemi, kayıt defteri ve ağ etkinlikleri açısından incelemektedir. Analiz ortamı sanal makinelerle izole edilerek yapılandırılmış; VMware Workstation Pro üzerinde Windows 7 x64 SP1 işletim sistemi kullanılmış ve Process Explorer, Process Monitor, Autoruns, Regedit, Wireshark gibi araçlarla izleme yapılmıştır. Yazarlar, fidye yazılımının mssecsvc.exe ile başlatıldığını ve ardından tasksche.exe, @WanaDecryptor@.exe, taskdl.exe, taskse.exe gibi alt süreçlerle çok aşamalı bir enfeksiyon süreci yürüttüğünü gözlemlemişlerdir. Dinamik analiz sırasında şifrelenmiş dosyaların oluşturulması, kayıt defterine kalıcılık amacıyla yeni anahtarlar eklenmesi ve ".WNCRYT" uzantılı dosyalarla orijinal dosyaların silinmesi gibi etkiler detaylı şekilde kaydedilmiştir. Ağ analizinde, fidye yazılımının önce "kill-switch" alan adını sorguladığı, ardından MS17-010 güvenlik açığını kullanarak SMB üzerinden yayılım sağladığı ve DoublePulsar arka kapısını kurarak sisteme kalıcı erişim elde ettiği tespit edilmiştir. Ayrıca, farklı DoublePulsar komutları (ping, exec) ve SMB paketlerinin içerdiği özel alanlardaki saklı veriler analiz edilerek fidye yazılımının ağ üzerinden nasıl haberleştiği açıklanmıştır. Son olarak, elde edilen Göstergeler (IOCs) YARA kurallarına dönüştürülerek, zararlı yazılım tespiti ve paylaşımı amacıyla kullanılabilecek siber tehdit istihbaratı çıktıları üretilmiştir. Çalışma, WannaCry'nin farklı katmanlarda bıraktığı izleri ortaya koyarak zararlı yazılımlara karşı bilgi paylaşım temelli savunma yaklaşımlarına katkı sunmaktadır.

M. Satheesh Kumar, Jalel Ben-Othman ve K.G. Srinivasagan tarafından yazılan WannaCry Fidye Yazılımı ve Tespiti Üzerine Bir Araştırma (An Investigation on Wannacry Ransomware and its Detection) başlıklı makale[3], WannaCry fidye yazılımının bir incelemesini yapar. Makale, fidye yazılımlarının kökeninin 1989 yılındaki PC Cyborg Trojan'a dayandığını, bu yazılımın kurbanın sistemini kilitleyerek 189 dolarlık bir fidye talep ettiğini belirtir. Yazarlar, fidye yazılımlarını, kurbanın sisteme erişimini engelleyen

"Kilitleyici (Locking) Ransomware" ve yalnızca dosyaları şifreleyen "Kripto (Crypto) Ransomware" olmak üzere iki sınıfa ayırmaktadır. WannaCry'nin analizinde, yazılımın yayılmak için Microsoft'un SMB protokolündeki MS17-010 güvenlik açığından ve bu açığı istismar eden "EternalBlue" aracından faydalandığı vurgulanmaktadır. Yazılımın içerisinde bulunan "taskdl.exe", "mssecsv.exe" gibi dosya adları ve "WNCry@2017" gibi dizelerden oluşan Yara kuralları ile ağ trafiğinde WannaCry'nin kullandığı DoublePulsar ve EternalBlue istismarlarını tespit etmeye yönelik Snort kuralları gibi savunma mekanizmaları sunulmuştur.

Maxat Akbanov, Vassilios G. Vassilakis ve Michael D. Logothetis'in WannaCry Fidyeye Yazılımı: Enfeksiyon, Kalıcılık, Kurtarma Önleme ve Yayılma Mekanizmalarının Analizi (WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms) makalesi ise[4], WannaCry'ı özel olarak kurulmuş bir sanal laboratuvar ortamında dinamik analize tabi tutarak incelemektedir. Bu metodoloji sayesinde, yazılımın enfeksiyon, kalıcılık, kurtarmayı önleme ve yayılma aşamalarındaki davranışları adım adım gözlemlenmiştir. Analiz, WannaCry'nin sistemde kalıcılık sağlamak için kendisini "Microsoft Security Center (2.0) Service" (mssecsvs2.0) adıyla bir hizmet olarak kaydettiğini ve hem Windows kayıt defterine hem de AutoRun özelliğine eklediğini ortaya koymuştur. Makalenin veri kurtarmayı engellemek için kullanılan kesin komutları deşifre etmiştir. Çalışma yazılımın içindeki parola korumalı ZIP arşivinin şifresinin "WNCry@2017" olduğunu bulmuş ve her kurban için oluşturulan özel RSA anahtarının, kurtarılmasını önlemek amacıyla kullanıldıktan sonra bellekten silindiğini (CryptDestroyKey fonksiyonu ile) göstermiştir. Son olarak, yayılma trafiği incelendiğinde, SMB tarama paketlerinin içerisinde sabit kodlanmış iki adet IP adresinin (192.168.56.20 ve 172.16.99.5) gömülü olduğu keşfedilmiştir, bu da ağ tabanlı tespit için önemli bir ipucu sunmaktadır.

3. Ransomware'ın Tanımı ve Tarihçesi

3.1. Ransomware Tanımı

Ransomware (fidye yazılımı), bilgisayar sistemine bulaştıktan sonra verileri şifreleyen veya kullanıcı erişimini engelleyen bir zararlı yazılım türüdür; saldırgan, verilerin açılması veya sistemin yeniden işlev kazanması karşılığında fidye (genellikle kripto para) talep eder.

IBM, fidye yazılımlarını şifreleme temelli ve kilitleme temelli olmak üzere iki ana gruba ayırmıştır. İlk grup dosyaları güçlü şifreleme algoritmaları (Advanced Encryption Standard, RSA vb.) ile kilitleyerek kullanılmaz hale getirirken, ikincisi sadece ekran kilidi veya sistem blokajı oluşturur.

3.2. Ransomware Tarihçesi

Ransomware tarihte ilk olarak 1989 yılında Joseph Popp tarafından geliştirilen AIDS Trojan (bilinen adıyla PC Cyborg) ile ortaya çıkmıştır. Bu ransomware'ın çalışma mantığı, kullanıcıya sisteme yeniden erişim için nakit ödeme talep etmesidir.

2000'li yıllarda Archiveus (2006) ve GPcode (2006) gibi ilk şifreleme temelli ransomware örnekleri görülmüştür. 2009 yılında Rusya'da ortaya çıkan bir "kilitleme" yazılımı, 2010 yılında bir küresel tehdit haline gelmiştir.

Tüm bu gelişmelere rağmen, yine de asıl ransomware tehdidi 2013'te CryptoLocker ile patlak vermiştir diyebiliriz. CryptoLocker, bulaştığı bilgisayardaki dosyaları AES/RSA şifrelemiş ve şifrelenen veriler karşılığında fidye olarak Bitcoin ödemesi istemiştir. Bu gelişmeler yanında Bitcoin gibi anonim ödeme araçlarının da kullanılması fidye saldırılarını hızlandırmış, WannaCry (Mayıs 2017) ve NotPetya (Haziran 2017) gibi küresel salgınlarla büyük zararlar verilmiştir.

4. Ransomware'in Çalışma Prensipleri

4.1. Bulaşma

Saldırganlar genellikle ortalama e-postaları, sahte bağlantılar veya drive-by indirme gibi yöntemlerle kullanıcının bilgisayarına kötü amaçlı yazılımı bulaştırabilir. Ayrıca güvenlik güncellemelerindeki açıklarla veya uzaktan masaüstü protokollerinin sahip olduğu bazı açıklar aracılığıyla da kurbanın sistemine yayılabilir.

4.2. Yayılma

Fidye yazılımları sistemde çalıştırıldıklarında, genellikle ağ üzerindeki diğer cihazlara; Spear Phishing, SMB açıkları, RDP Brute Force gibi yöntemlerle veya ağ üzerinde paylaşılan ortak dosyalar aracılığıyla bulaşarak yayılırlar. Örneğin WannaCry, EternalBlue açığına kullanarak aynı ağı kullanan makinelerle otomatik olarak bulaşmıştır.

4.3. Şifreleme

Ransomware, hedef bilgisayardaki değerli dosyaları (belgeler, resimler, veritabanları vb.) güçlü AES/RSA gibi şifreleme algoritmaları ile şifreler.

AES (Advanced Encryption Standard, Türkçe adıyla Gelişmiş Şifreleme Standartı), elektronik verinin şifrelenmesi için sunulan bir standarttır. AES ile tanımlanan şifreleme algoritmasında, hem şifreleme hem de şifreli metni çözmede kullanılan anahtarlar birbiriyle aynı olur. Bu durum, sadece şifreleyen kişinin dosyaları çözebilmesine olanak tanır.

RSA, güvenliği tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanan bir tür açık anahtarlı şifreleme yöntemidir. Bir RSA kullanıcısı, iki büyük asal sayının çarpımını üretir ve seçtiği diğer bir değerle birlikte ortak anahtar olarak ilan eder. Seçilen asal çarpanları ise saklar. Ortak anahtarı kullanan biri herhangi bir mesajı şifreleyebilir, ancak şu anki yöntemlerle eğer ortak anahtar yeterince büyükse sadece asal çarpanları bilen kişi bu mesajı çözebilir.

Tüm bunları dikkate aldığımızda; ortalama bir kullanıcının, bu gibi algoritmalar ile şifrelenen dosyaları çözmesi ve kurtarması imkansızdır.

4.4. Fidye Notu

Şifreleme veya kilitleme işlemi sonrasında ekranda veya dosyalar arasında fidye notu görünür. Bu notta kurbanın nasıl ve nereye ödeme yapacağı (genellikle fidye Bitcoin gibi bir kripto para olarak istenir ve ekranda yatırılması istenen cüzdan adresi yer alır) ve belirli süre içinde ödenmemesi durumunda verilerin silineceği ya da ifşa edileceği bildirilir. Çoğu saldırıda fidye ödendiğinde deşifre anahtarı verilir, ancak tamamen güvenilir değildir.

4.5. RaaS (Ransomware-as-a-Service) Tanımı

Ransomware-as-a-Service, fidye yazılımlarının geliştiriciler tarafından hazırlanıp, genellikle dark web üzerinden istekte bulunan potansiyel saldırganlara kiralandığı veya satıldığı bir iş modelidir. Bu model yasal değildir ama tıpkı yasal yazılım hizmetleri gibi çalışır; burada hizmet veren taraf ransomware geliştiricileri, müşteri ise saldırganlardır.

RaaS sistemleri sayesinde teknik bilgisi olmayan kişiler bile kolayca ransomware saldırıları düzenleyebilir. Bu durum, siber tehditlerin yayılmasını ciddi oranda artırmıştır.

5. Yaygın Saldırı Türleri ve Örnekleri

Ransomware'lar kilitleme (locker) veya şifreleme (crypto) temelli olabilir. Kilitleme, sistemi veya ekranı kilitleyerek erişim engeller. Şifreleme, dosyaları alışılagelmiş şifreleme algoritmalarıyla kilitler. Ancak bazı yazılımlar, yapılan saldırılar ile veri yok etme (wiper) amacı taşıyabilir (ör. NotPetya 2017).

5.1. Örnek Saldırıları

CryptoLocker (2013): İlk büyük çaplı şifreleme saldırısıdır. Kullanıcıların sisteme girmesiyle bilgisayarı tarayıp dosyaları şifrelemiş, Bitcoin ile ödeme talep etmiştir.

WannaCry (Mayıs 2017): SMB açığından yararlanarak yayılan “ransomworm” türünün örneğidir. İngiltere’de 80’den fazla NHS kuruluşunu hedeflemiş, 20.000’i aşkın doktor randevusu iptal edilmiştir.

NotPetya (Haziran 2017): İlk başta fidye yazılımı olarak görüldüyse de, gerçekte kurban verilerini geri getirmeyi imkânsız kılan yıkıcı bir saldırıydı. Bu etkisinden dolayı en fazla zarar ettiren saldırılardan biridir.

Maze (2019): Çift şantaj (şifrelemeye ek olarak çalınan verileri açığa çıkarmayla da tehdit ederek fidye istemiştir.) taktiğiyle öne çıktı. Bu yöntem, günümüzde REvil, Conti gibi büyük fidye grupları tarafından yaygınlaşmıştır.

LockBit, BlackCat, Hive vb.: Bu RaaS grupları son yılların en aktif fidye yazılımlarındandır. Örneğin LockBit ve BlackCat büyük şirketleri hedefleyen saldırılar düzenlemiş; Hive ise FBI’nın 2022’deki operasyonu ile çökertilmiştir.

Tedarik Zinciri Saldırıları: MOVEit 2023 açığı aracılığıyla BBC ve British Airways gibi kurumlar saldırıya uğramıştır.

6. Ransomware Saldırılarının Etkileri

6.1. Ekonomik Etkiler

Fidye saldırıları şirketlere büyük mali kayıp yaşatmıştır. IBM’in Cost of Data Breach raporuna göre 2023’te ortalama bir fidye yazılımı ihlali maliyeti 5,13 milyon dolardır, bir önceki yıla göre bu maliyet %13 artıştır. Chainalysis, 2023’te fidye ödemelerinin 1 milyar doları geçtiğini raporlamıştır. Başka bir örnek olarak MGM Resorts’un 2023’te LockBit saldırısına uğraması sonucu fidyeyi ödememesine rağmen tahmini zararı 100 milyon doları aşmıştır. Şirketler bu saldırılar sonucu oluşan iş kayıpları, veri kurtarma giderleri ve itibar zedelenmesi gibi nedenler ile ciddi ekonomik baskı altına girerler.

6.2. Toplumsal Etkiler

Fidye saldırıları sağlık, altyapı ve kamu hizmetlerini doğrudan etkileyebilme potansiyeline sahiptir. Örneğin 2017'deki WannaCry salgını sonucu İngiltere'deki hastanelerde acil hizmetler aksadı, randevular iptal edildi ve ambulanslar başka bölgelere sevk edildi. Bu durum, WannaCry saldırısının sağlık hizmetini doğrudan etkilediğine dair çarpıcı bir örnektir. Benzer şekilde şehir yönetimleri, okullar ve diğer kamusal kurumlar da fidye saldırılarından olumsuz etkilenmiştir. Büyük altyapıya yönelik saldırılar ulusal güvenlik boyutuna ulaşabilmekte, vatandaşları paniğe sevk edebilmektedir.

6.3. Bireysel Etkiler

Fidye saldırılarında bireysel kullanıcılar da büyük risk altında olabilirler. Örneğin CryptoLocker gibi yazılımlar akademik çalışmaları veya aile fotoğraf ve videolarını kilitleyebilir. Bu tarz saldırılarda kaybedilen verilerin geri gelmemesi bireylere hem maddi hem manevi büyük zararlar verebilir. Kurbanlar uzun süreli emek harcanmış belgelerini kaybetme tehlikesiyle karşılaşır ve psikolojik olarak yenilirler. Bu da onları çaresiz bıraktığı için panik yapmalarına ve saldırganlara fidye ödemelerine iter.

7. Korunma ve Müdahale Yöntemleri

7.1. Altyapı Güvenliği

Kurumlar ve bireysel kullanıcılar, yazılım ve işletim sistemlerini güncel tutmalıdır; güvenlik açıklarını kapatmak için sık sık yamaları yüklemelidir. Çok faktörlü kimlik doğrulama (MFA) kullanılmalıdır. Ağ içinde kritik sistemler segmentlere ayrılmalı, RDP gibi gereksiz uzaktan erişimler kapatılmalıdır.

7.2. Eğitim ve Farkındalık

Çalışanlara ve bireylere, ortalama e-postalarına karşı dikkatli olmaları için eğitim verilmeli; e-posta ekleri ve şüpheli bağlantılar açmama konusunda bilinçlendirme sağlanmalıdır.

7.3. Yedekleme

Periyodik olarak yedekleme yapılmalıdır. Veriler mutlaka offline ve şifreli yedeklerle tutulmalı; bu yedekler düzenli olarak test edilmelidir.

7.4. Tespit ve Müdahale

Anti-virüs ve davranış tabanlı tespit sistemleri ile anormal şifreleme faaliyetleri izlenmelidir. Bir saldırı tespit edilirse hemen izolasyon (etkilenen cihazların ağdan çıkarılması) yapılmalı ve olay müdahale planı devreye sokulmalıdır. Ekipler, saldırıdan etkilenen sistemleri yedekten geri yüklemeye hazır olmalıdır.

7.5. Raporlama ve İşbirliği

Olay anında ilgili kurumlara (CISA ve ulusal siber birimlere) bildirim yapılmalıdır. Hukuki kurumlar saldırıların takibi ve çetelerin çökertilmesi için iş birliği yapmaktadır.

7.6. Ödeme Politikası

En son çare olarak fidye ödemesi görülmelidir. Birçok güvenlik kurumu, ödemeyi önermemektedir ve bu durumun suçluları cesaretlendireceğini ve suça teşvik edeceğini

vurgulamaktadır. Kesinlikle ödeme yapmamayı tercih eden kuruluşlar, yedeklerden devam etmek yönünde karar alırlar.

8. Statik Analiz

Bir dosyanın çalıştırılmadan sadece binary dosyasından elde edilen sonuçlardan yola çıkarak değerlendirilmesine static analiz denir . Bu kısımda WannaCry virüsünün static olarak analiz edilmesi anlatılmıştır.

8.1. Virustotal Sonuçları

Elimizdeki WannaCry örneğinin Virustotal sonuçlarına ulaşmak için öncelikle powershell üzerinde [Get-FileHash](#) komutu kullanılarak dosyanın hashi alınmıştır.

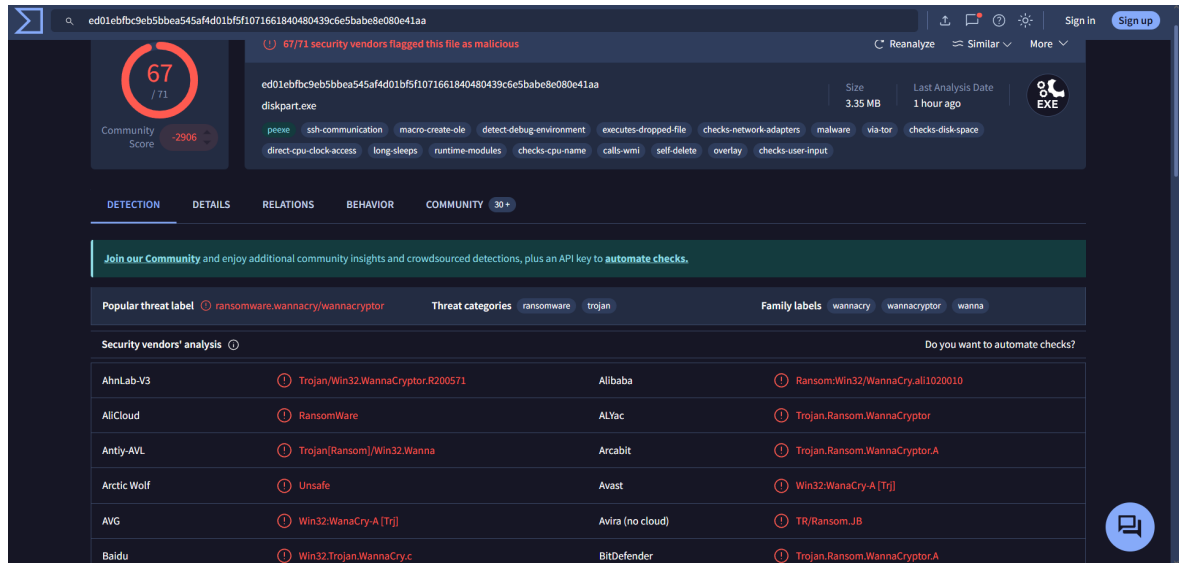
```
PS C:\Users\victim\desktop> Get-FileHash ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe.malv | Format-List

Algorithm : SHA256
Hash       : ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA
Path       : C:\Users\victim\desktop\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe.malv
```

Böylelikle dosyanın SHA-256 hashine ulaşıyoruz.

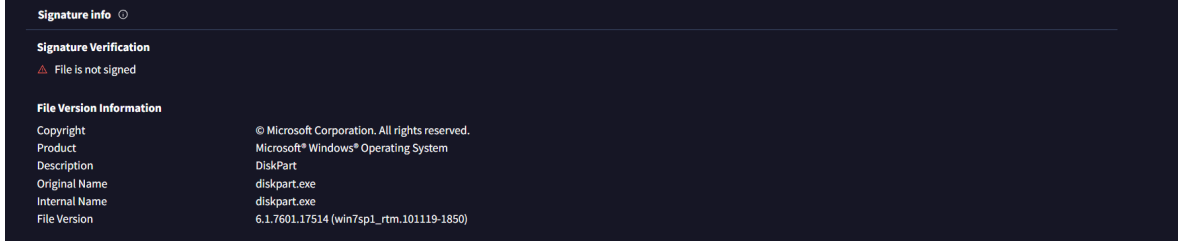
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

Bu hash kullanılarak Virustotal üzerinden arama yapılmıştır.



71 security vendor analizinden 67 sinin bunu zararlı yazılım olarak tanımladığı görülüyor. Pek çoğu zararlı yazılımı doğrudan ismiyle tanımlamayı başarıyor.

Aynı zamanda burada dosyanın orijinal adının `diskpart.exe` olduğunu görüyoruz. Saldırganlar dikkat çekmemek için system32 de bulunan ve windowsa ait olan `diskpart.exe` isimli dosyayı taklit etmeye çalışmışlar.



Burada da dosya versiyon bilgilerinin saldırganlar tarafından windows dosyası gibi gösterilmek amacıyla manipüle edilmiş olduğunu görüyoruz. Fakat yukarıda dosyanın imzalı olmadığı gösteriliyor. Bu da dosyanın gerçekten windows dosyası olmadığını gösterir.

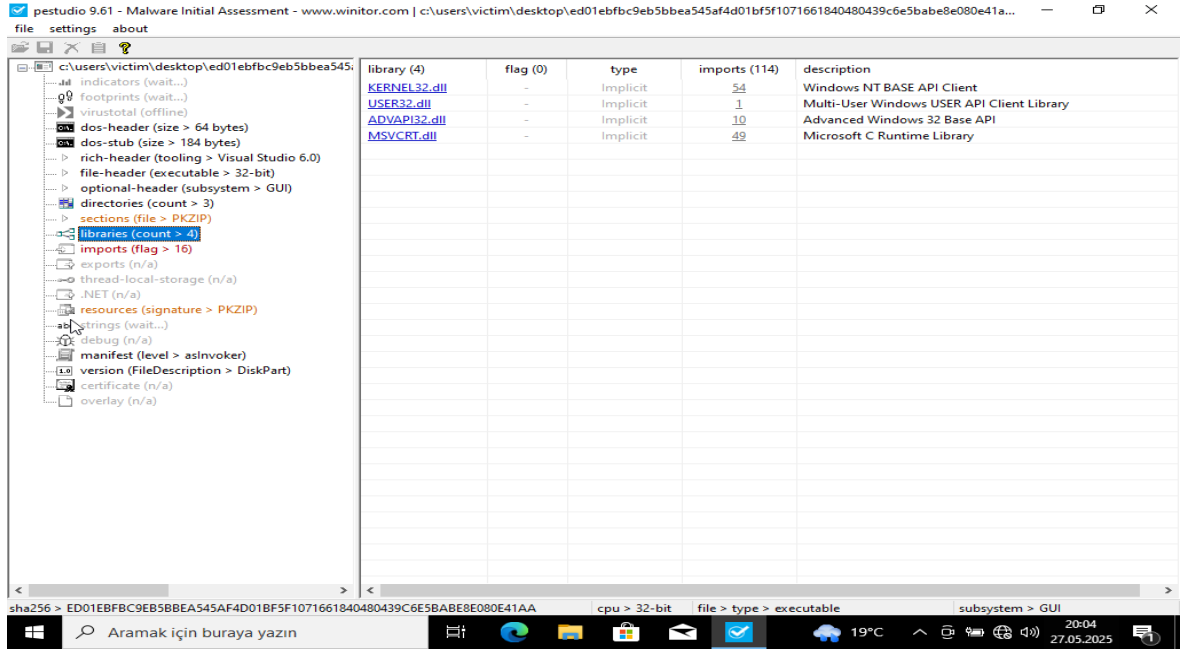


Burada dosyanın farklı hash çeşitleri, dosya boyutu, dosya tipi oluşturulma tarihi vb. gibi genel bilgiler görüyoruz.

Not : 2010 olarak belirtilen oluşturma zamanı virüsün gerçek yayılma tarihiyle çelişkili duruyor. Bu sebeple bu bilginin de manipüle edilerek değiştirildiğini var sayabiliriz.

8.2. PESTudio ile Analiz

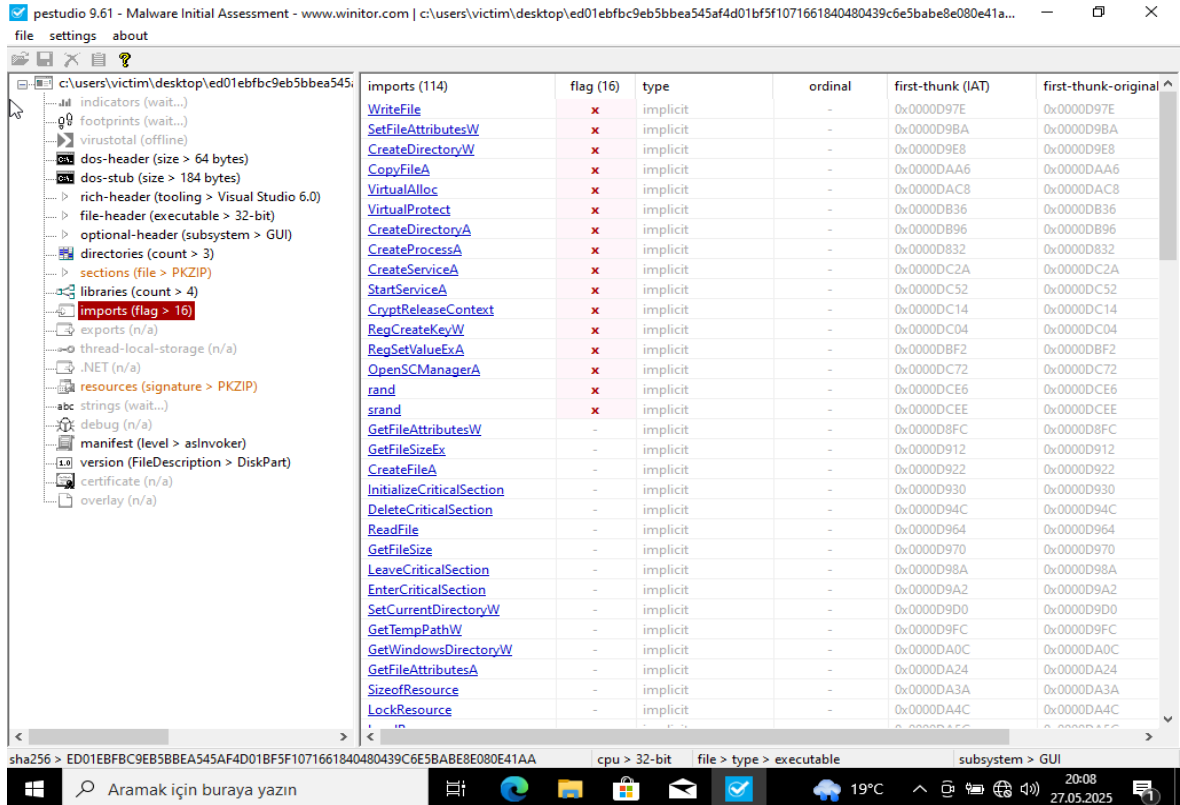
Zararlı yazılım PESTudio uygulaması kullanılarak analiz edilmiştir.



Burada zararlı yazılımın kullandığı kütüphaneler gösterilmiştir.

KERNEL32.dll USER32.dll ADVAPI32.dll MSVCRT.dll

İsimli 4 kütüphane kullanıldığı görülmüştür.



Burada ise kullandığı çağrılar gösterilmiştir. Buradaki çağrılar analiz edilerek virüsün davranışları hakkında bilgi edinilebilir. Dosya veya klasör yaratma, kopyalama, silme gibi işlemler yapıyor olduğu görünüyor. CryptoDecrypt, CryptoEncrypt, CryptoDestroyKey gibi

çağrılarla şifreleme yapıldığını daha sonra ise anahtarın silindiğini görüyoruz. RegCreateKey ile persistence mekanizması sağlanıyor olabilir.

Bu tarz şüpheli çağrılar virüsün zararlı davranışları hakkında ipucu veriyor.

8.3. String Analizi

Cihazımızda PESTudio string kısmında sorun olduğu için (sürekli waitingde takılı kalıyor) farklı araçlar kullanarak yazılımın string bilgilerini çıkarttık.

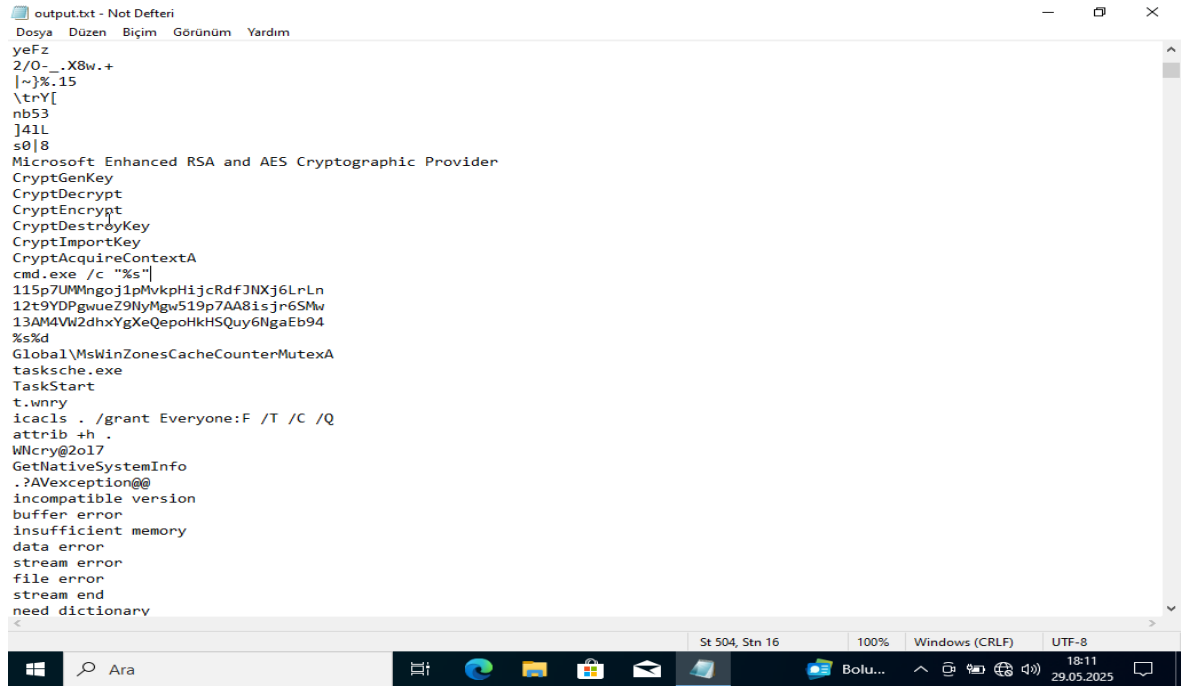
Floss ve String kullandık her ikisi de aynı çıktıyı veriyor.

```
C:\Users\victim\Desktop\Strings>strings.exe ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe.malv > output.txt

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
```

Yukarıdaki komut ile string uygulaması kullanılarak virüsün stringi output.txt isimli text dosyasına yazılmıştır.

Bu işlemle binary kodundan çıkarılabilecek bütün string verileri çıkartılıyor. Böylelikle yukarıda da gördüğümüz kütüphaneler ve çağrılar da dahil olmak üzere bitcoin cüzdanları, programın çalıştıracığı bazı komutlar, oluşturacağı dosyalar, kullanacağı uzantılar, dil seçenekleri vb.. bir çok bilgiye erişme şansımız oluyor.



```
output.txt - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
yeFz
2/O_..X8w.+
|~}%15
\trY[
nb53
]41L
s0|8
Microsoft Enhanced RSA and AES Cryptographic Provider
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
cmd.exe /c "%s"
115p7UMMngoj1pMvkhHjCRdFJNXj6LrLn
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
13AM4VW2dhxYgXeQepoHkHSQuy6NGaEb94
%$%d
Global\MSWinZonesCacheCounterMutexA
tasksche.exe
TaskStart
t.wnry
icacls . /grant Everyone:F /T /C /Q
attrib +h .
WNcry@2o17
GetNativeSystemInfo
.?AVException@@
incompatible version
buffer error
insufficient memory
data error
stream error
file error
stream end
need dictionary
```

Yukarıda cmd ile bir komut çalıştırıldığını görüyoruz fakat komutun ne olduğu hemen yanında değil muhtemelen bir değişkene atanmış.

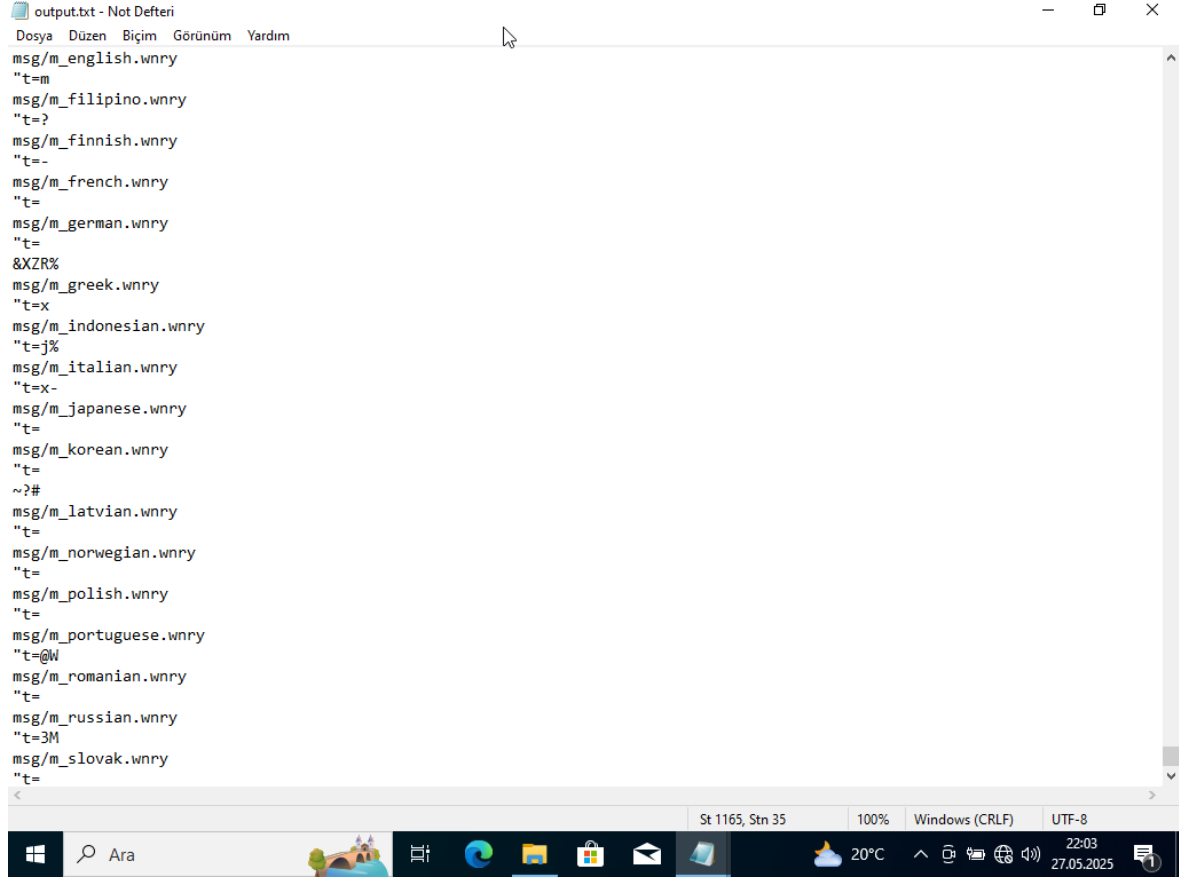
Hemen altında 3 adet bitcoin cüzdanı görülüyor.

Tasksche.exe şeklinde bir dosya ismi görülüyor virüsün bu isimde bir dosya oluşturmasını veya bu isimde bir dosyaya ulaşmaya çalışmasını bekleyebiliriz.

icacs . /grant everyone: F /T /C /Q komutu ile bütün dosyalar üzerinde tam izne sahip olmayı amaçlıyor.

attrib +h . kullanarak bulunduğu dizini gizlemeye çalışıyor.

GetNativeSystemInfo komutu ile sistem hakkında bilgi alıyor.



```
output.txt - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
msg/m_english.wnry
"t=m
msg/m_filipino.wnry
"t=?
msg/m_finnish.wnry
"t=-
msg/m_french.wnry
"t=
msg/m_german.wnry
"t=
&XZR%
msg/m_greek.wnry
"t=x
msg/m_indonesian.wnry
"t=j%
msg/m_italian.wnry
"t=x-
msg/m_japanese.wnry
"t=
msg/m_korean.wnry
"t=
~?#
msg/m_latvian.wnry
"t=
msg/m_norwegian.wnry
"t=
msg/m_polish.wnry
"t=
msg/m_portuguese.wnry
"t=@W
msg/m_romanian.wnry
"t=
msg/m_russian.wnry
"t=3M
msg/m_slovak.wnry
"t=
```

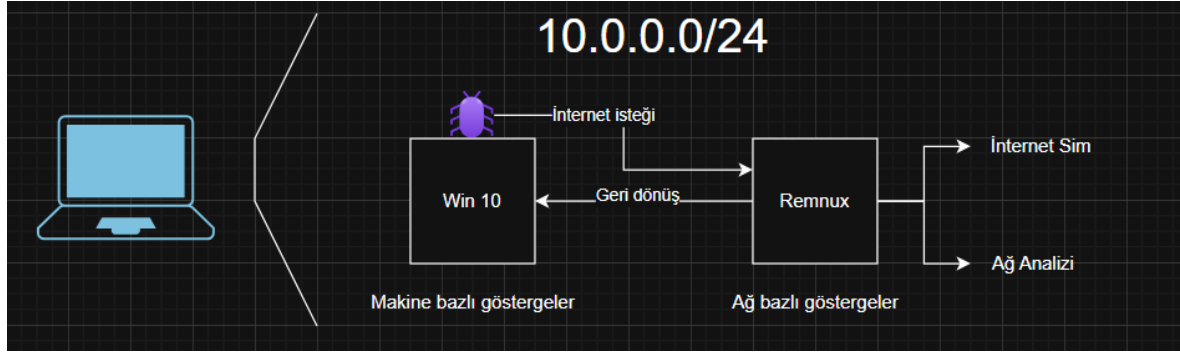
Burada virüsün çalışabileceği diller görülüyor.

9. Dinamik Analiz

9.1. Analiz Ortamının Kurulumu

Zararlı yazılım analizi, yüksek riskler barındıran bir süreçtir. Analiz edilen yazılımın, özellikle de WannaCry gibi ağ solucanı(worm) yeteneklerine sahip bir fidye yazılımının, kontrol dışına çıkarak ana makineye veya yerel ağa sızması, telafisi zor sonuçlar doğurabilir. Projede, bu tehlikeden kaçınmak ve analizin tamamen güvenli sınırlar içinde kalmasını sağlamak amaçlanmıştır. Bu amaçla, tüm analiz süreci dış dünyadan ve ana sistemden tamamen yalıtılmış, kapalı bir sanal laboratuvar ortamında yürütülmüştür. Bu izole ortam, zararlı yazılımın tüm faaliyetlerini serbestçe gerçekleştirmesine olanak tanır ve yayılma riskini sıfıra indirerek güvenli bir şekilde gözlem yapılmasını sağlar. Bu kontrollü ortam Oracle VirtualBox ile oluşturulmuştur. Laboratuvar, iki temel sanal makineden oluşacak şekilde tasarlanmıştır: Birincisi, WannaCry'nin doğrudan üzerine kurulup çalıştırılacağı, yani "kurban" rolünü üstlenecek olan Windows 10 bir sanal makinedir. İkincisi ise, kurban makinenin ağ ve sistem davranışlarını izlemek, trafiğini yakalamak ve analiz etmek için

kullanılacak olan, içerisinde çok sayıda siber güvenlik ve tersine mühendislik aracı barındıran özel bir Linux dağıtımı olan Remnux sanal makinesidir.



Bu iki sanal makinenin birbirleriyle iletişim kurabilmesi ancak dış dünya ile hiçbir şekilde temas edememesi için VirtualBox üzerinde özel bir ağ yapılandırması gerçekleştirilmiştir. Yapılandırmada, sanal makinelerin ağ bağdaştırıcıları için "Yalnızca Ana Makine Bağdaştırıcısı (Host-Only Adapter)" seçeneği kullanılarak özel bir iç ağ oluşturulmuştur. Bu ağ modu, sanal makinelerin yalnızca birbirleriyle ve ana makineyle iletişim kurabildiği, ancak ana makinenin internete çıktığı fiziksel ağ arayüzüne (Wi-Fi veya Ethernet) erişemediği kapalı bir devre yaratır. Bu sayede tam bir izolasyon sağlanmıştır. Oluşturulan bu iç ağda, DHCP sunucusu aracılığıyla IP adreslemesi yapılmıştır.

Yapılan yapılandırma sonucunda Remnux analiz makinesi 10.0.0.3 IP adresini alırken, Windows 10 kurban makinesi 10.0.0.4 IP adresini almıştır. Bu yapılandırmanın ve izolasyonun başarısı, basit ancak etkili bir testle doğrulanmıştır. Windows 10 makinesi üzerinden çalıştırılan ping 10.0.0.3 komutu, Remnux makinesine başarıyla ulaşıldığını ve iç ağ iletişiminin sorunsuz çalıştığını göstermiştir. Bunun hemen ardından, ping 8.8.8.8 komutu ile Google'ın genel DNS sunucusuna bir istek gönderilmiş ve bu isteğin zaman aşımına uğrayarak başarısız olduğu gözlemlenmiştir.

```
Komut İstemi

C:\Users\tetik>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3b19:6542:fc47:d77c%8
    IPv4 Address. . . . . : 10.0.0.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Users\tetik>ping 8.8.8.8

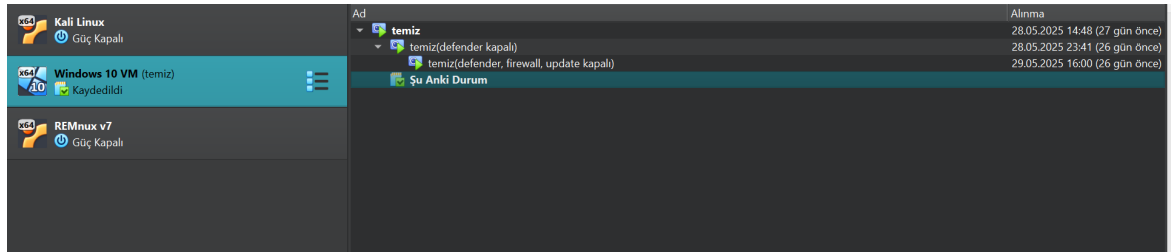
Pinging 8.8.8.8 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\tetik>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:
Reply from 10.0.0.3: bytes=32 time=1ms TTL=64
Reply from 10.0.0.3: bytes=32 time<1ms TTL=64
```

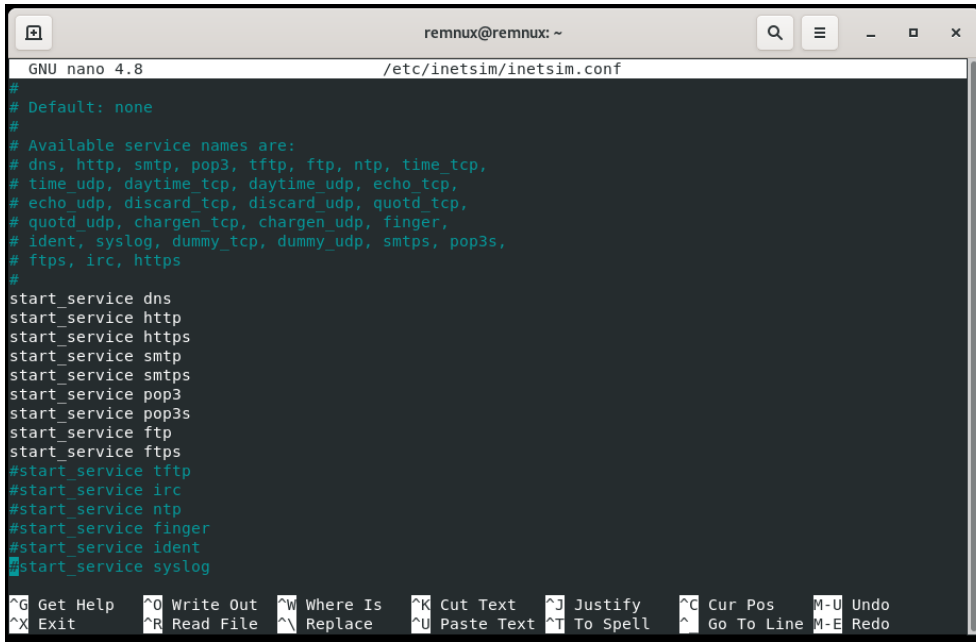
WannaCry analizinde testlerin tekrarlanabilirliğini sağlamak ve her teste temiz bir sistemle başlamak için VirtualBox'ın "Snapshot (Anlık Görüntü)" özelliği kullanılmıştır. WannaCry'ı çalıştırmadan önce, temiz ve yapılandırılmış Windows 10 sanal makinesinin anlık görüntüleri alınmıştır. Analiz tamamlandıktan sonra bu anlık görüntüye geri dönülerek sanal makinenin durumu ilk temiz haline getirilmiştir.



9.2. Ağ Davranışlarının Simülasyonu

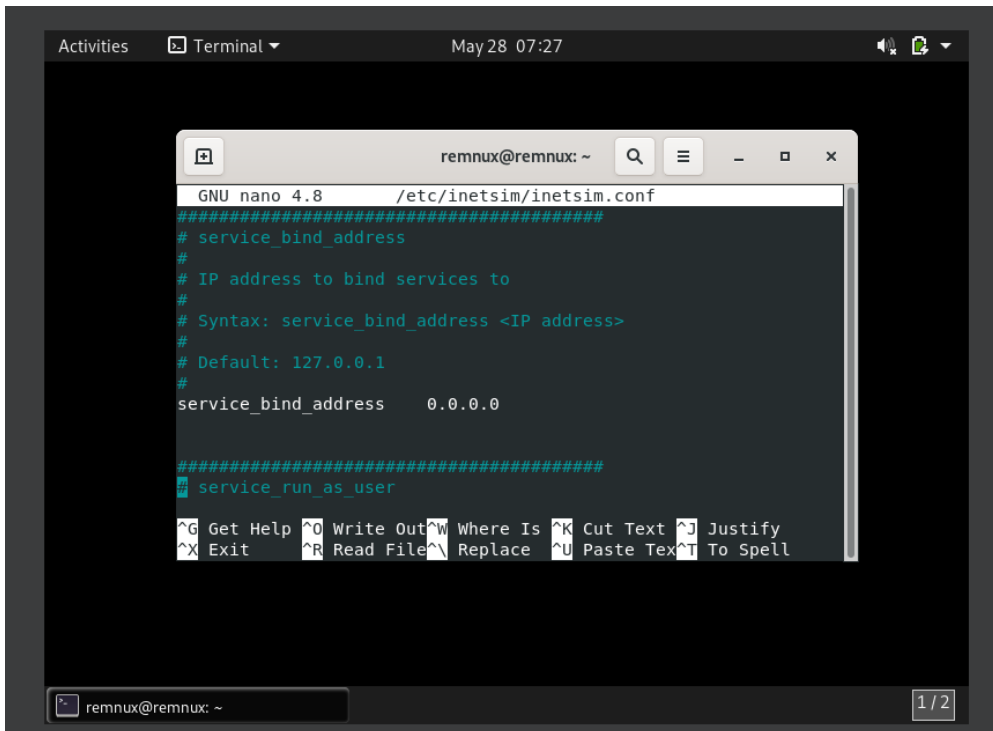
WannaCry, bulaştığı sistemde aktif hale gelmeden önce bir internet bağlantısının varlığını kontrol eder. Eğer bir internet bağlantısı tespit edemezse, analiz edildiğini veya bir sandbox ortamında olduğunu varsayarak bazı fonksiyonlarını çalıştırmayabilir ya da tamamen pasif kalabilir. WannaCry'ın ağ üzerindeki yayılma ve iletişim kurma davranışlarını eksiksiz bir şekilde gözlemleyebilmek için, onun gerçek bir internet ağına bağlı olduğuna inandırılması gerekiyor. Projenin bu aşamasında, Windows 10 makinesini internete çıkarmadan, ona sahte bir internet ortamı hazırlanmıştır. Bu simülasyonu gerçekleştirmek için Remnux analiz makinesi üzerine INetSim (Internet Services Simulation Suite) aracı kurulmuş ve yapılandırılmıştır. INetSim, DNS, HTTP, HTTPS, FTP, SMTP gibi yaygın internet protokollerini taklit edebilen güçlü bir araçtır. WannaCry bir internet sitesine bağlanmaya veya bir alan adını çözümlemeye çalıştığında, INetSim bu isteği karşılayarak sahte bir yanıt üretir ve zararlı yazılımın analiz ortamında tam olarak çalışmasını sağlar.

INetSim'in doğru çalışması için /etc/inetsim/inetsim.conf yolundaki yapılandırma dosyasında değişiklikler yapılmıştır. Öncelikle start_service dns ifadesi yorum satırı olmaktan çıkartarak dns servisini aktifleştirilmiştir.



```
remnux@remnux: ~  
GNU nano 4.8 /etc/inetsim/inetsim.conf  
# Default: none  
#  
# Available service names are:  
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,  
# time_udp, daytime_tcp, daytime_udp, echo_tcp,  
# echo_udp, discard_tcp, discard_udp, quotd_tcp,  
# quotd_udp, chargen_tcp, chargen_udp, finger,  
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,  
# ftps, irc, https  
#  
start_service dns  
start_service http  
start_service https  
start_service smtp  
start_service smtps  
start_service pop3  
start_service pop3s  
start_service ftp  
start_service ftps  
#start_service tftp  
#start_service irc  
#start_service ntp  
#start_service finger  
#start_service ident  
start_service syslog  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo  
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo
```

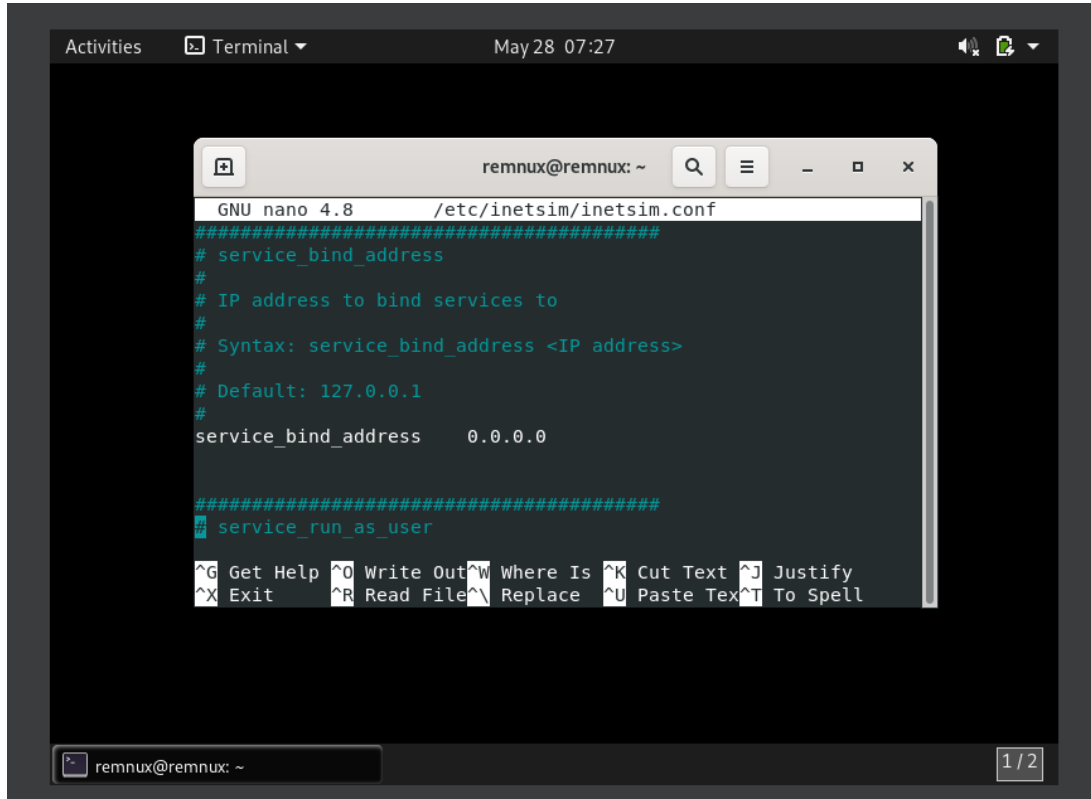
Varsayılan olarak INetSim yalnızca kendi üzerindeki (localhost) istekleri dinler. Ancak projede, Windows 10 makinesinden gelen istekleri de dinlemesi gerekiyor. Bu nedenle, `service_bind_address` parametresi `0.0.0.0` olarak değiştirilmiştir. Bu ayar, INetSim'in Remnux makinesine bağlı tüm ağ arayüzlerindeki istekleri dinlemesini sağlayarak Windows 10 makinesiyle iletişim kurmasına olanak tanımıştır.



```
Activities Terminal May28 07:27  
remnux@remnux: ~  
GNU nano 4.8 /etc/inetsim/inetsim.conf  
#####  
# service_bind_address  
#  
# IP address to bind services to  
#  
# Syntax: service_bind_address <IP address>  
#  
# Default: 127.0.0.1  
#  
service_bind_address 0.0.0.0  
#####  
# service_run_as_user  
#  
# Syntax: service_run_as_user <user>  
#  
# Default: root  
#  
service_run_as_user root  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify  
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell  
remnux@remnux: ~ 1/2
```

Yapılan yapılandırmalardan bir diğeri de DNS hizmetiyle ilgilidir. `dns_default_ip` parametresi, Remnux makinesinin kendi IP adresi olan `10.0.0.3` olarak ayarlanmıştır. Bu yapılandırma, Remnux makinesini kurban makine için bir nevi sahte DNS sunucusuna dönüştürür. Windows 10 makinesi üzerindeki WannaCry, herhangi bir alan adını çözümlmek için bir DNS isteği gönderdiğinde, bu istek Remnux'a ulaşır ve INetSim, bu

alan adının IP adresinin 10.0.0.3 olduğuna dair sahte bir yanıt döner. Bu yönlendirme sayesinde, zararlı yazılımın sonraki tüm HTTP veya diğer protokol bağlantı denemeleri, gerçek bir sunucu yerine doğrudan bizim analiz makinemize yönlendirilmiş olur.



The screenshot shows a terminal window titled 'remnux@remnux: ~' with a date and time of 'May 28 07:27'. Inside the terminal, a nano editor is open editing the file '/etc/inetsim/inetsim.conf'. The editor shows the following configuration:

```
GNU nano 4.8 /etc/inetsim/inetsim.conf
#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 0.0.0.0

#####
# service_run_as_user
#
#####
```

At the bottom of the nano editor, there is a status bar with the following text: '^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify', '^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell'. The terminal window also shows a '1 / 2' indicator at the bottom right.

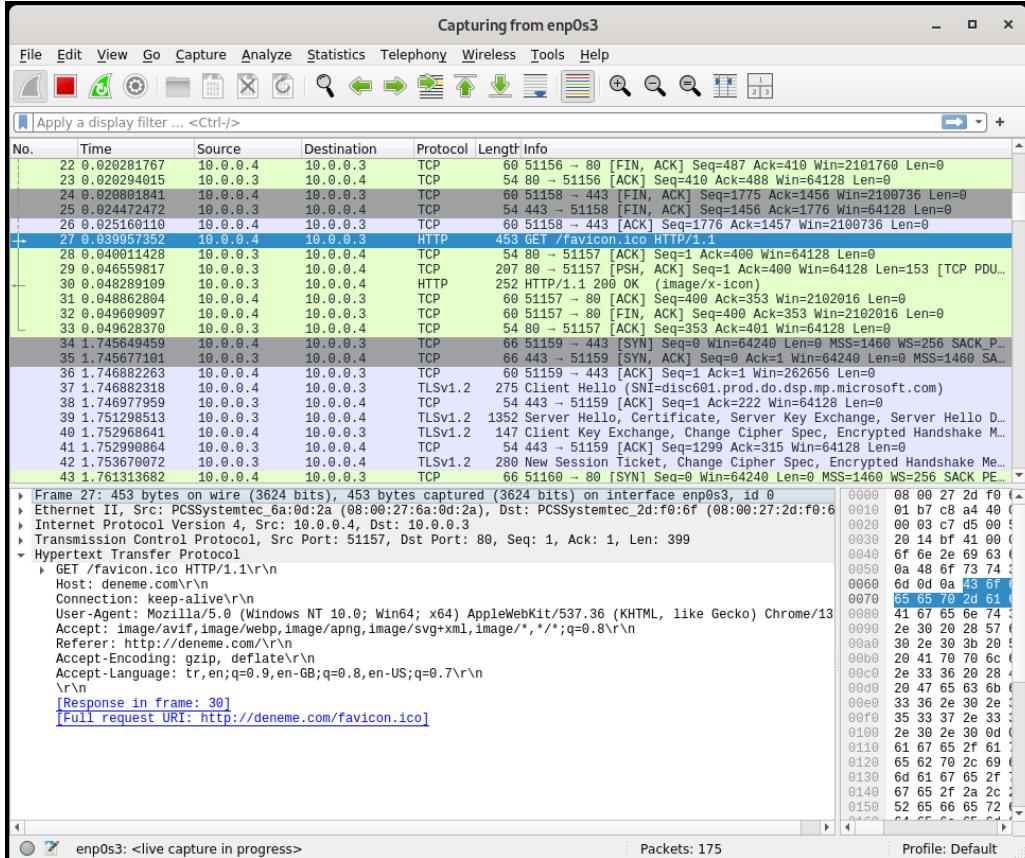
Bu sahte internet altyapısı kurulduktan sonra, Remnux bash üzerinde inetsim komutu kullanılarak başlatılır. WannaCry'ın tüm ağ iletişim denemelerini kaydetmek ve izlemek için Remnux üzerinde ağ trafiği analiz araçları çalıştırılmıştır. Hem komut satırı tabanlı TCPDump hem de grafik arayüzlü Wireshark araçları kullanılmıştır. Bu paket analizörleri, Windows 10 makinesinden Remnux makinesine doğru akan her bir veri paketini yakalar, protokollerine göre ayırtmış ve detaylı bir şekilde sunar.

TCPDump aracı, host 10.0.0.4 and port 80 or port 443 filtresiyle çalıştırılmıştır. Bu filtreleme ile kurban makineye (10.0.0.4) ait olan ve standart web protokolleri olan HTTP (port 80) ile HTTPS (port 443) üzerinden geçen paketlerle sınırlandırılmıştır. Paket içeriğinin okunabilir metin formatında görüntülenmesi için -A parametresi ve paketlerin veri kaybı olmadan tam olarak yakalanması -s 0 parametresiyle kullanılmıştır. Yakalanan bu veri akışı, boru hattı (|) operatörü aracılığıyla grep "Host:" komutuna yönlendirilmiştir ve tcpdump tarafından üretilen tüm metin içerisinde yalnızca hedeflenen sunucu adını belirten "Host:" başlığını içeren satırların ayıklanmasını sağlamıştır.

```
remnux@remnux: ~/code
remnux@remnux: ~
remnux@remnux: ~
remnux@remnux: ~/code

remnux@remnux:~/code$ sudo tcpdump -s 0 -l -A host 10.0.0.4 and port 80 or port 443 | grep "Host:"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
Host: deneme.com
Host: deneme.com
```

Ağ trafiğinin daha detaylı ve görsel bir analizi için grafik arayüzlü bir protokol analiz aracı olan Wireshark'tan da faydalanılmıştır. Remnux makinesi üzerinde çalıştırılan Wireshark, kurban makineden gelen tüm paketleri gerçek zamanlı olarak yakalayarak protokol katmanlarına göre ayrıştırılmış bir biçimde sunmuştur.



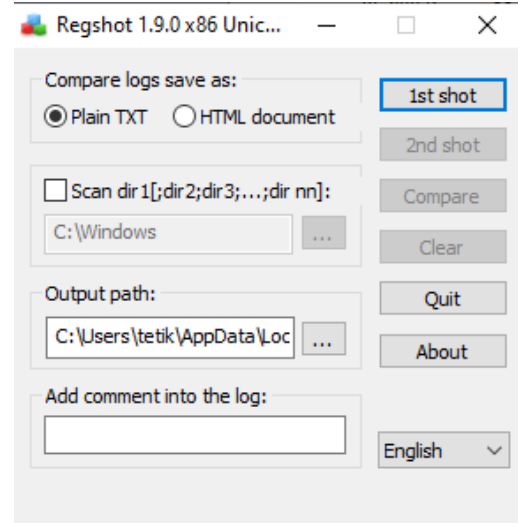
9.3. Host Bazlı Davranışlar

Virüsün bulaştığı "host" yani kurban sistem üzerinde ne gibi değişiklikler yaptığı detaylı bir şekilde incelenmiştir. Bu inceleme, zararlı yazılımın sistemde nasıl kalıcılık sağladığını, hangi dosyaları hedef aldığını ve sistem bütünlüğünü nasıl bozduğunu ortaya çıkarır. WannaCry'nın Windows 10 makinesi üzerindeki dosya sistemi, Windows Kayıt Defteri (Registry) ve proses aktiviteleri üzerindeki etkilerini gözlemlenmiştir.



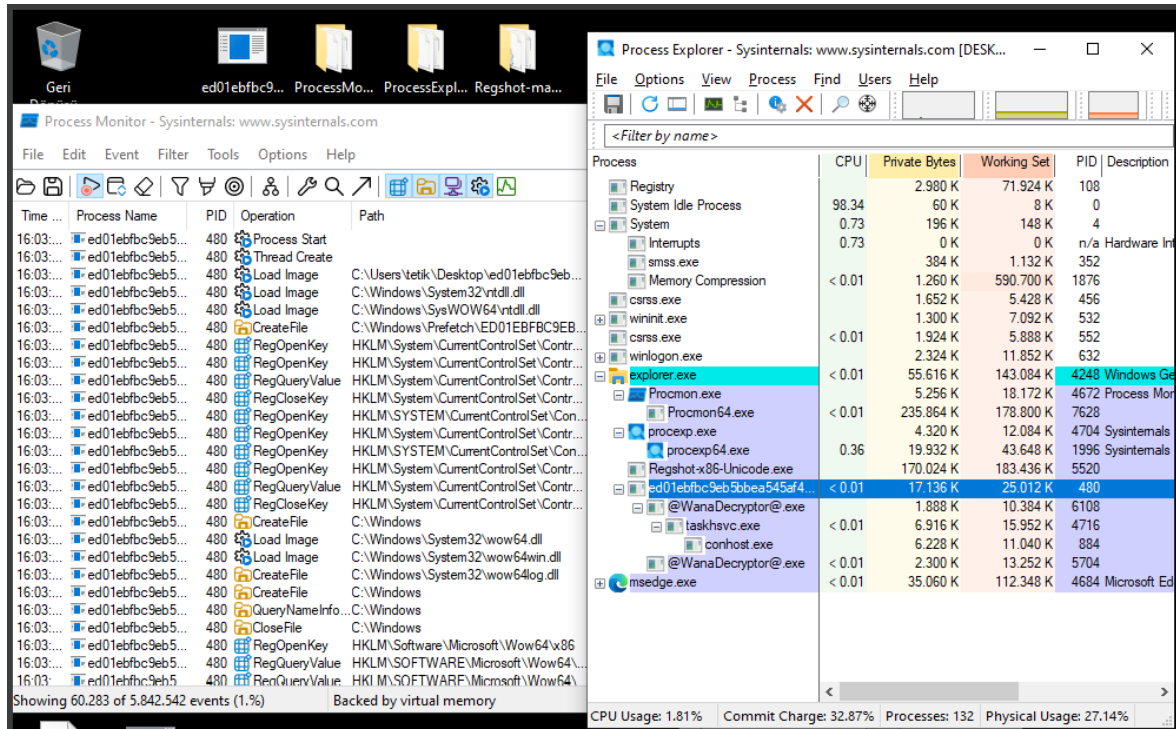
Sistemdeki değişiklikleri tespit etmek için sistemin önceki ve sonraki durumlarını karşılaştıran Regshot aracı kullanılmıştır. Regshot, temel olarak sistemin iki farklı zamandaki anlık görüntüsünü alarak aradaki farkları raporlayan bir programdır.

Analiz sürecinde, WannaCry çalıştırılmadan hemen önce, Regshot kullanılarak tüm Windows Kayıt Defteri'nin ve C:\ sürücüsündeki dosya yapısının ilk anlık görüntüsü ("1st shot") alınmıştır. Daha sonra, WannaCry'nin sisteme bulaşıp şifreleme işlemlerini tamamlaması beklendikten sonra, Regshot ile ikinci bir anlık görüntü ("2nd shot") daha alınmıştır. İki görüntü karşılaştırıldığında, WannaCry tarafından oluşturulan yeni dosyalar, uzantısı değiştirilen veya şifrelenen kullanıcı dosyaları ve yazılımın sistem her başladığında yeniden çalışmasını sağlamak için Kayıt Defteri'ne eklediği kalıcılık (persistence) anahtarları net bir şekilde ortaya çıkarılmıştır.



```
~res-x86 - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
-----
Keys deleted: 1
-----
HKU\S-1-5-21-3693231751-3370521027-845009403-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData
-----
Keys added: 12
-----
HKLM\SOFTWARE\WanaCrypt0r
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\ASR Writer
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\ASR Writer
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\COM+ REGDB Writer
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\Registry Writer
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\Shadow Copy Optimization Writer
HKU\S-1-5-21-3693231751-3370521027-845009403-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Applicatio
HKU\S-1-5-21-3693231751-3370521027-845009403-1001\SOFTWARE\Classes\Local Settings\MrtCache\C:%5CProgram Files%5CWindowsApps%5
HKU\S-1-5-21-3693231751-3370521027-845009403-1001_Classes\Local Settings\MrtCache\C:%5CProgram Files%5CWindowsApps%5CMicrosof
-----
Values deleted: 2
-----
HKU\S-1-5-21-3693231751-3370521027-845009403-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\Microsoft.Win
HKU\S-1-5-21-3693231751-3370521027-845009403-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\windows.immer
-----
Values added: 20
-----
HKLM\SOFTWARE\Microsoft\EdgeUpdate\RetryAfter: 0x6838E69F
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ksvbg1qy551: ""C:\Users\tetik\Desktop\tasksche.exe""
HKLM\SOFTWARE\WanaCrypt0r\wd: "C:\Users\tetik\Desktop"
HKLM\SYSTEM\ControlSet001\Control\Session Manager\PendingFileRenameOperations: 5C 00 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 55
00 78 00 74 00 00 00 00 5C 00 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 74 00 65 00 74 00 6
00 00 00 5C 00 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 74 00 65 00 74 00 69 00 68 00 5C 00
<
St 1, Stn 1 100% Windows (CRLF) UTF-16 LE
16:05 29.05.2025
```

Sistemdeki anlık aktiviteleri ve proses davranışlarını gerçek zamanlı olarak izlemek için ise Sysinternals Suite içerisinde yer alan Procmon (Process Monitor) ve Process Explorer araçları kullanılmıştır. Process Explorer, çalışan tüm işlemleri hiyerarşik bir ağaç yapısında göstererek, WannaCry'nin ana prosesinin hangi alt prosesleri başlattığını ve bu proseslerin sisteme etkilerini anlık olarak izleme imkanı sunmuştur. Procmon ise, sistemde gerçekleşen olayları kaydeder. Procmon bu veri yığınına filtreleme özelliğine sahiptir. Analiz sırasında filtreler, yalnızca WannaCry'a ait prosesin aktivitelerini gösterecek şekilde ayarlanmıştır. Bu sayede, WannaCry'nin hangi sırayla hangi dosya türlerini aradığı, bunları nasıl okuyup şifrelediği ve sonuna .WNCRY gibi uzantıları nasıl eklediği gibi davranışları, bir zaman çizelgesi üzerinde adım adım izlenebilmiştir.



9.4. Sonuç

Yapılan gözlemlerde, analiz edilen bu sürümün, WannaCry saldırılarının aksine bir "kill-switch" alan adına sorgu yapmadığı ve herhangi bir harici sunucuya veya web sitesine bağlantı kurma girişiminde bulunmadığı tespit edilmiştir. Yazılım sistem üzerindeki kullanıcı dosyalarını hedef alarak dosya oluşturma, silme ve mevcut dosyaları değiştirme yoluyla şifrelemiştir. Regshot aracıyla yapılan kayıt defteri karşılaştırması fidyeye yazılımı, kalıcılık sağlamak ve sistem her yeniden başlatıldığında kendisini tekrar çalıştırmak amacıyla HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run kayıt defteri yoluna "ksvqblqy551" gibi rastgele isimlendirilmiş yeni bir öğe eklemiştir.

10. Kaynakça

1. S. -C. Hsiao and D. -Y. Kao, "The static analysis of WannaCry ransomware," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea (South), 2018, pp. 153-158, doi: [10.23919/ICACT.2018.8323680](https://doi.org/10.23919/ICACT.2018.8323680).
2. D. -Y. Kao and S. -C. Hsiao, "The dynamic analysis of WannaCry ransomware," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea (South), 2018, pp. 159-166, doi: [10.23919/ICACT.2018.8323682](https://doi.org/10.23919/ICACT.2018.8323682).
3. M. Satheesh Kumar, J. Ben-Othman and K. G. Srinivasagan, "An Investigation on Wannacry Ransomware and its Detection," 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 2018, pp. 1-6, doi: [10.1109/ISCC.2018.8538354](https://doi.org/10.1109/ISCC.2018.8538354).
4. M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms", JTIT, vol. 75, no. 1, pp. 113–124, Mar. 2019, doi: [10.26636/jtit.2019.130218](https://doi.org/10.26636/jtit.2019.130218).
5. KPMG Türkiye, "Fidyeye Yazılımı (Ransomware) Nedir?," KPMG Türkiye, Ağu. 2022. <https://kpmg.com/tr/tr/home/insights/2022/08/fidyeye-yazilimi-ransomware.html>

6. K. Laffan, "A Brief History of Ransomware," Varonis, 9 Haz. 2023. <https://www.varonis.com/blog/a-brief-history-of-ransomware>
7. K. Baker, "Introduction to Ransomware," CrowdStrike, 4 Mar. 2025. <https://www.crowdstrike.com/blog/introduction-to-ransomware>
8. S. Fox-Sowell, "Ransomware incidents rose 73% globally in 2023, report shows," Statescoop, 26 Eyl. 2024. <https://statescoop.com/ransomware-incidents-rose-73-globallyin-2023-report-shows/>
9. Chainalysis Team, "Ransomware Hit \$1 Billion in 2023," Chainalysis, 7 Şub. 2024. <https://www.chainalysis.com/blog/ransomware-2024/>
10. Coveware, "Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022," Coveware, 28 Tem. 2022. <https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-asmedium-ransom-falls-in-q2-2022>
11. Cybersecurity and Infrastructure Security Agency (CISA), "#StopRansomware Guide: Ransomware and Data Extortion," CISA, Eyl. 2023. <https://www.cisa.gov/stopransomware/ransomware-guide>
12. J. Holdsworth and M. Kosinski, "What is Ransomware as a Service?," IBM Security Intelligence, 5 Eyl. 2024. <https://securityintelligence.com/posts/ransomware-as-a-service/>
13. IBM Security, "Cost of a Data Breach Report 2023," IBM, 2023. <https://www.ibm.com/downloads/cas/EXK6XEKG>
14. Ermaner & Karabay Avukatlık, "TÜRK CEZA KANUNU MADDE 244 BAĞLAMINDA RANSOMWARE YAZILIMLARI VE CRYPTOLOCKER VİRÜSÜ," Ermaner & Karabay Avukatlık, 16 Kas. 2020. <https://ermaner.av.tr/turk-ceza-kanunu-madde-244-baglaminda-ransomware-yazilimleri-ve-cryptolocker-virusu/>
15. Akamai, "What is Maze Ransomware?," Akamai. <https://www.akamai.com/tr/tr/resources/glossary/what-is-maze-ransomware>
16. H. Bates, "7 Ransomware Predictions for 2025: From AI Threats to Targeted Attacks," Zscaler, 29 Oca. 2025. <https://www.zscaler.com/blogs/research/7-ransomwarepredictions-2025>
17. Federal Bureau of Investigation, "Ransomware: Prevention and Response," IC3.gov, 2020. <https://www.ic3.gov/Media/PDF/2020IC3Brochures/Ransomware%20and%20You.pdf>
18. A. Hern, "WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017," The Guardian, 30 Ara. 2017. <https://www.theguardian.com/technology/2017/dec/30/wannacrypetya-notpetya-ransomware>