T.C.
DÜZCE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

FİDYE YAZILIMLARIN DENEYSEL ANALİZİ

BAHATTİN DOĞAN

YÜKSEK LİSANS TEZİ
ELEKTRİK ELEKTRONİK VE BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMAN
PROF. DR. RESUL KARA

DÜZCE, 2020

T.C.
DÜZCE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

FİDYE YAZILIMLARIN DENEYSEL ANALİZİ

Bahattin DOĞAN tarafından hazırlanan tez çalışması aşağıdaki jüri tarafından Düzce Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik ve Bilgisayar Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Prof. Dr. RESUL KARA

Düzce Üniversitesi

Eş Danışman

Dr. Öğr. Üyesi ERKAN ÇETİNER

Zonguldak Bülent Ecevit Üniversitesi

Jüri Üyeleri

Prof. Dr. RESUL KARA
Düzce Üniversitesi _____

Dr.Öğr. Üyesi A. Talha KABAKUŞ
Düzce Üniversitesi _____

Dr. Öğr. Üyesi Şafak KAYIKÇI
Bolu Abant İzzet Baysal Üniversitesi _____

Tez Savunma Tarihi: 07/09/2020

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

07 Eylül 2020

Bahattin DOĞAN

TEŞEKKÜR

Yüksek lisans öğrenimimde ve bu tezin hazırlanmasında gösterdiği her türlü destek ve yardımdan dolayı çok değerli hocam Prof. Dr. RESUL KARA'ya ve ders aldığım tüm hocalarıma en içten dileklerimle teşekkür ederim.

Tez çalışmam boyunca değerli katkılarını esirgemeyen eş danışmanım Dr. Öğr. Üyesi ERKAN ÇETİNER'e de şükranlarımı sunarım.

Bu çalışma boyunca yardımlarını ve desteklerini esirgemeyen sevgili aileme ve çalışma arkadaşlarıma sonsuz teşekkürlerimi sunarım.

07 Eylül 2020 **Bahattin DOĞAN**

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ vii

ÇİZELGE LİSTESİ ix

ÖZET x

ABSTRACT xi

1. GİRİŞ 1

1.1. TEZİN KAPSAMI 1
1.2. LİTERATÜR ARAŞTIRMASI 4
1.3. TEZİN ORGANİZASYONU 7

2. FİDYE YAZILIMLARI 8

2.1. FİDYE YAZILIMLARININ TARİHİ 11
2.2. FİDYE YAZILIM TÜRLERİ 13
2.3. EN ETKİLİ FİDYE YAZILIMLARI 15
2.3.1. GoldenEye 15
2.3.2. WannaCry 15
2.3.3. Cryptolocker 15
2.3.4. Locky 15
2.3.5. Petya 16
2.3.6. Powerware 16
2.3.7. zCrypt 16
2.4. KULLANICILARA GÖNDERİLEN FİDYE YAZILIMI ÖRNEKLERİ 16
2.4.1. Örnek 1: Fiyat Teklif E-Postaları 16
2.4.2. Örnek 2: Özgeçmiş veya İş Başvurusu Yapan E-Postalar 17
2.4.3. Örnek 3: Locky Fidye Yazılımı Oltalama E-Postası 18
2.4.4. Örnek 4: GrandCrab Yayılma Mekanizması 19
2.4.5. Örnek 5: Kargo Takip Uygulaması 19
2.4.6. Örnek 6: Fatura E-Postaları 20
2.5. ANALİZ YÖNTEMLERİ 20

3. deneysel analiz ortamı hazırlama 23

3.1. REMNUX ANALİZ ORTAMININ HAZIRLANMASI 23
3.2. CUCKOO SANDBOX ANALİZ ORTAMININ HAZIRLANMASI 33

4. ZARARLI YAZILIM ANALİZLERİ 45

4.1. REMNUX İLE NETWORK TABANLI ZARARLI YAZILIM ANALİZİ 45
4.2. CUCKOO SANDBOX İLE WANNACRY ZARARLI YAZILIM ANALİZİ 49
4.2.1. Analiz Özet Bilgileri 52
4.2.2. Statik Analiz Bilgileri 54
4.2.3. Davranış Analiz Bilgileri 55
4.3. CUCKOO SANDBOX İLE PETYA ZARARLI YAZILIM ANALİZİ 59
4.3.1. Analiz Özet Bilgileri 61
4.3.2. Statik Analiz Bilgileri 63

4.3.3. Davranış Analiz Bilgileri 65
5. ZARARLI VE ZARARSIZ YAZILIMLARIN ANALİZ SONUÇLARININ KARŞILAŞTIRILMASI 68
6. SONUÇLAR VE ÖNERİLER 72
7. KAYNAKLAR 73
ÖZGEÇMİŞ 77

ŞEKİL LİSTESİ

Sayfa No

Şekil 2.1. Fidye yazılımını bilgisayar üzerinde çalışma yapısı..... 9
Şekil 2.2. Fiyat teklif e-posta örneği..... 17
Şekil 2.3. İş başvurusu için özgeçmiş e-posta örneği..... 18
Şekil 2.4. Locky fidye yazılımı e-posta örneği..... 18
Şekil 2.5. GrandCrab fidye yazılımı e-posta örneği..... 19
Şekil 2.6. Kargo takip ile oltalama e-posta örneği..... 19
Şekil 2.7. Fatura ile oltalama e-posta örneği..... 20
Şekil 3.1. Remnux analiz ortamı topolojisi..... 24
Şekil 3.2. Virtualbox sürüm bilgisi..... 25
Şekil 3.3. Remnux ova dosyasının import edilmesi..... 25
Şekil 3.4. Remnux ram bellek gösterimi..... 26
Şekil 3.5. Remnux sanal bilgisayar temel görünümü..... 26
Şekil 3.6. Remnux genel bilgi penceresi..... 27
Şekil 3.7. Remnux sistem penceresi temel ayarları..... 27
Şekil 3.8. Remnux ekran ayarları..... 28
Şekil 3.9. Remnux nat özellikli ethernet gösterimi..... 28
Şekil 3.10. Remnux host-only ethernet gösterimi..... 29
Şekil 3.11. Root kullanıcısına geçiş temel komutları..... 29
Şekil 3.12. Remnux ağ ayarları gösterimi..... 30
Şekil 3.13. Remnux iptables komutları gösterimi..... 30
Şekil 3.14. Remnux iptables dosya içeriği ve kayıt edilmesi..... 31
Şekil 3.15. Remnux inetsim ayar dosyası..... 31
Şekil 3.16. Remnux inetsim servis çalıştırılması..... 32
Şekil 3.17. Remnux fakedns servis çalıştırılması..... 32
Şekil 3.18. Wireshark görünümü..... 32
Şekil 3.19. Cuckoo sandbox analiz ortamı ağ topolojisi..... 33
Şekil 3.20. Ubuntu 16.04 iptables konfigürasyon dosyası..... 39
Şekil 3.21. Cuckoo servisinin çalıştırılması..... 40
Şekil 3.22. Cuckoo web serverın çalıştırılması..... 40
Şekil 3.23. Cuckoo sandbox giriş penceresi..... 41
Şekil 3.24. İstemci güvenlik duvarı ayarları..... 41
Şekil 3.25. İstemci ağ ayarları..... 42
Şekil 3.26. İstemci Python sürüm bilgisi..... 42
Şekil 3.27. İstemci Python-Pillow kurulumu..... 43
Şekil 3.28. İstemci antivirüs ayarları..... 43
Şekil 3.29. İstemci kullanıcı hesap denetim ayarları..... 44
Şekil 3.30. İstemci agent.py çalıştırılması..... 44
Şekil 4.1. Wireshark DNS bilgileri..... 46
Şekil 4.2. WannaCry kilitleme ve bilgilendirme penceresi..... 47
Şekil 4.3. WannaCry ARP sorguları..... 47
Şekil 4.4. WannaCry ağdaki diğer bilgisayarlara SMB ile bağlantı kurulması..... 48
Şekil 4.5. WannaCry bulaşma öncesi ve sonrası çalışan ağ servisleri..... 49
Şekil 4.6. WannaCry başlangıçta etkilenen ülkeler[47]..... 51
Şekil 4.7. Cuckoo ile Wannacry analizi özet penceresi..... 53
Şekil 4.8. Cuckoo ile Wannacry analizi http isteği..... 53
Şekil 4.9. Cuckoo ile Wannacry statik analiz bilgileri..... 54

Şekil 4.10. Cuckoo ile Wannacry statik analizi string bilgileri. 55
Şekil 4.11. Cuckoo ile Wannacry analizi virustotal sonuçları. 55
Şekil 4.12. Cuckoo ile Wannacry davranışsal analiz bilgileri. 56
Şekil 4.13. Cuckoo ile Wannacry analizi registry değişiklikleri. 57
Şekil 4.14. Cuckoo ile Wannacry analizi dosya işlemleri. 57
Şekil 4.15. Cuckoo ile Wannacry analizi network işlemleri..... 58
Şekil 4.16. Cuckoo ile Wannacry analizi process işlemleri..... 58
Şekil 4.17. Cuckoo ile Wannacry analizi senkronizasyon işlemleri..... 59
Şekil 4.18. Cuckoo ile Wannacry analizi ağ işlemleri..... 59
Şekil 4.19. Petya chkdsk görünümü..... 60
Şekil 4.20. Petya kilitleme ve bilgilendirme penceresi..... 61
Şekil 4.21. Cuckoo ile Petya analizi özet penceresi. 61
Şekil 4.22. Cuckoo ile Petya analizi virustotal sonuçları. 62
Şekil 4.23. Cuckoo ile Petya statik analiz bilgileri. 63
Şekil 4.24. Cuckoo ile Petya dll dosya bilgileri..... 64
Şekil 4.25. Cuckoo ile Petya statik analizi string bilgileri..... 64
Şekil 4.26. Cuckoo ile Petya analizi virustotal sonuçları. 65
Şekil 4.27. Cuckoo ile Petya davranışsal analiz bilgileri..... 65
Şekil 4.28. Cuckoo ile Petya analizi dosya işlemleri..... 66
Şekil 4.29. Cuckoo ile Petya analizi process işlemleri. 66
Şekil 4.30. Cuckoo ile Petya analizi senkronizasyon işlemleri. 67

ÇİZELGE LİSTESİ

Sayfa No

Çizelge 3.1. Remnux analiz ortamı ip adres bilgileri. 24
Çizelge 3.2. Cuckoo sandbox analiz ortamı ip adres bilgileri. 33
Çizelge 3.3. Cuckoo kurulumu hazırlık komutları 34
Çizelge 3.4. Tcpdump kurulum komutları..... 35
Çizelge 3.5. Yara kurulum komutları 38
Çizelge 5.1. Analiz edilen yazılımların genel bilgileri. 68
Çizelge 5.2. Yazılımların analiz özeti bilgileri. 69
Çizelge 5.3. Yazılımların statik analiz bilgileri. 70
Çizelge 5.4. Yazılımların davranışsal analiz bilgileri. 71
Çizelge 5.5. Yazılımların ağ hareket bilgileri. 71

ÖZET

FİDYE YAZILIMLARIN DENEYSEL ANALİZİ

Bahattin DOĞAN
Düzce Üniversitesi
Fen Bilimleri Enstitüsü, Elektrik Elektronik ve Bilgisayar Mühendisliği Anabilim Dalı
Yüksek Lisans Tezi
Danışman: Prof. Dr. Resul KARA
Eylül 2020, 76 sayfa

Zararlı yazılım, bilişim sistemlerinde kullanıcının bilgisi dışında işletim sistemlerine bulaşan, istenmeyen değişiklikler yaparak işleyişi bozan, yetkisiz verilere erişim elde eden, şifreleyen, sistem üzerinde tahribata yol açan, istenmeyen reklamlar gösteren, siber suçlular tarafından yazılan kötü niyetli yazılımlardır. Günümüz dünyasında siber tehditler katlanarak artış göstermektedir. Siber dünyadaki en büyük tehditlerden biri, milyonlarca bilgisayarı etkileyen fidye yazılımı (ransomware) saldırılarıdır. Fidye yazılımları, benzersiz ve yıkıcı özellikleri ile günümüzün en önemli tehditleri arasına girmiştir. Bu çalışmada kötü amaçlı yazılımların yol açabileceği zararların statik ve dinamik olarak incelenmesi, analizinin daha kolay ve hızlı yapılabilmesi amacıyla kullanılmak üzere deneysel analiz ortamı yapılandırması gerçekleştirilmiştir. Kötü amaçlı yazılımların yol açabileceği zararların statik ve dinamik olarak incelenmesi, analizinin daha kolay ve hızlı yapılabilmesi amacıyla iki farklı çalışma ortamı birleştirilerek deneysel analiz ortamı oluşturulmuştur. Hazırlanan çalışma ortamı üzerinde dünyada yaygın olarak görülen ve önem arz eden fidye yazılımları ile iyi niyetli yazılımların çalışma ortamında deneysel analizleri yapılarak işletim sistemleri üzerinde oluşturduğu yıkıcı etkilerinin ortaya çıkardıkları sonuçlar karşılaştırılmıştır.

Anahtar sözcükler: Cuckoo, Fidye yazılımı, Kum havuzu, Remnux, Siber güvenlik.

ABSTRACT

EXPERIMENTAL ANALYSIS OF RANSOMWARE

Bahattin DOĞAN
Düzce University
Graduate School of Natural and Applied Sciences, Department of Electrical - Electronic and Computer Engineering
Master's Thesis
Supervisor: Prof. Dr. Resul KARA
September 2020, 76 pages

Malicious software is any software infecting operating systems beyond the user's knowledge in information systems, disrupting the working process by making unwanted changes, getting access to warrantless data, encrypting the system, causing destruction on the system, showing unwanted advertisements and being written by cybercriminals. Cyber threats have been increasing exponentially in today's world. Ransomware attacks are one of the most significant threats in the cyber world because of its unique and destructive characteristics. Furthermore, ransomware affects millions of computers. In this study, the potential damages caused by malicious software are examined both statically and dynamically in an experimental analysis environment formed to make the analysis more easily and quickly. The experimental analysis environment is created by combining two different study environments to examine the potential damages caused by malicious software both statically and dynamically, and to make the analysis more easily and quickly. Ransomware has gained prevalence worldwide and accordingly, has great importance. Ransomware and other types of software are analyzed, and the results produced by their destructive effects on operating systems are compared in the experimental analysis environment.

Keywords: Cuckoo, Cyber security, Ransomware, Remnux, Sandbox.

1. GİRİŞ

1.1. TEZİN KAPSAMI

Fidye, "yakalanan birini serbest bırakmak için belirli bir nihai hedefle ödenen nakit" ve "tutsak haldeki birinin esaretten kurtulabilmesi için talep edilen veya ödenen bir şey" olarak nitelendirilmektedir [1].

Sosyal mühendislik zafiyetleri, işletim sistemleri, bilgisayar programları ve zararlı yazılım önleyici programlardaki güvenlik zafiyetleri kullanılarak sistemlere bulaşan zararlı yazılımlar, pek çok farklı amaca hizmet etmektedir. Günümüz fidye yazılımı aileleri, gelişmiş şifreleme ve yayma şemaları uygulamaktadır. Kurban konumundaki kullanıcılara verileri kurtarmak amacıyla neredeyse sıfır ihtimal bırakılmaktadır.

Fidye yazılımı, "Fidye ödenmediği sürece sistem ekranını kilitleyerek veya kullanıcıların dosyalarını kilitleyerek kullanıcıların sistemlerine erişmelerini engelleyen, sınırlayan kötü amaçlı bir yazılım türü" olarak tanımlanmaktadır [2].

Günümüzde profesyonel suçlular tarafından siber terörizmden fidye istemeye kadar geniş bir uygulama alanı tasarlanmaktadır. Bu suçlular çok çeşitli yöntemler ve taktikler geliştirerek amaçlarına kolaylıkla ulaşmakta, bu duruma maruz kalma olasılığı kullanıcıların korkulu rüyası haline gelmektedir.

Teknolojinin gelişmesi ile birlikte teknolojik sistemlerin kullanımının artması, kötü niyetli insanlar için de yeni fırsatlar doğurmuştur. Önceleri bir kazanç kapısı olarak görülmeyen kötü amaçlı yazılımlar, günden güne çok büyük bir ticari sektör haline gelmiştir. Programcıların güvenlik zafiyetlerini önlemek için üretmiş oldukları yazılım güncellemeleri ve bilgisayar korsanlarının yazılımların getirmiş olduğu güvenlik açıklarını kullanarak yeni zararlı yazılım üretme amacı günümüzde kısır bir döngü oluşturmuştur.

Kötü amaçlı yazılım analizi, virüs, solucan, truva atı, rootkit veya arka kapı gibi belirli bir kötü amaçlı yazılım örneğinin işlevselliğini, kökenini ve potansiyel etkisini belirleme çalışması veya işlemidir.

Virüs bulaşmış makinenin temizlenmesi, çalışan sistemin arka planının keşfedilmesi,

sisteme devam eden bir saldırı varsa keşfedilmesi, saldırının ne zaman başladığı, saldırganın sistemdeki hedefinin ne olduğu, saldırı anında olaya müdahale edilmesi gibi durumlarda kötü amaçlı yazılımların analizinin yapılması gerekmektedir. Bu işlem ile yazılımın nasıl çalıştığı, hedefleri, etkilenen makineler, verilen hasar ölçülür ve kontrol edilir.

Fidye yazılımlarının tespiti ve engellenmesi, bu kötü amaçlı yazılım biçiminin büyük ölçüde genişlemesi nedeniyle son yıllarda çok aktif bir araştırma alanı haline gelmiştir. Bu doğrultuda zararlı yazılımların sistem üzerindeki etkilerini, üzerinde değişiklik yaptığı dosyaları, kurduğu bağlantıları analiz etmek amacıyla çalışma ortamı tasarımı yapılmıştır. Bu kapsamda iki farklı bölümden oluşan deneysel analiz ortamı tasarımı gerçekleştirilmiştir. Deneysel analiz ortamının ilk bölümü, iki ethernetli bir güvenlik duvarı (firewall) prensibi ile çalışan Remnux işletim sistemi ve istemci makinelerden oluşmaktadır. Bu yapıda istemci makinelerin tüm internet trafiği Remnux işletim sistemi üzerinden geçerek, sahte DNS, Http, Https, Ftp vb. servisler çalıştırılarak zararlı yazılımın ağ (network) analizi yapılmaktadır. Analiz ortamının ikinci bölümünde, Ubuntu işletim sistemi kurulu fiziksel bilgisayar üzerinde çalışan Cuckoo Sandbox ile kum havuzu kurulumu yapılandırılmakta ve istemci makineler virtualbox bağlantılı olarak bu kum havuzunda çalışmaktadır.

Fidye yazılımı tespiti için kullanılan teknikler fidye yazılımı eylemini iyi huylu yazılımdan ayırt etmeye dayanmaktadır. Fidye yazılımı özelliklerinin derinlemesine bir analizi, doğru bir algılama algoritması oluşturmak için çok önemlidir. Çalışmamızda gerçek kötü niyetli yazılım ve iyi niyetli yazılım örnekleri kullanılmıştır.

Bugün, Türkiye’de internet kullanımı 62 milyon kullanıcıya ulaşmış durumdadır [3]. İnternet, dünya çapında 3,7 milyar kullanıcıya hizmet vermektedir. Avrupa'da nüfusun %73,9'u ağa bağlı bilgisayarlar kullanmaktadır, Kuzey Amerika'da nüfusun %89'u interneti kullanmaktadır ve bu durum, dikkatli olmayan kullanıcılardan yararlanmak isteyen suçlular için bir hedef zenginliği ortamı oluşturmaktadır [4].

Fidye yazılımlar, maddi getirisi nedeniyle siber suçlular tarafından günümüzde yaygın olarak kullanılmakta ve kullanımı her geçen gün katlanarak artmaktadır. Fidye yazılımları genelde e-posta yolu ile bulaşmaktadır. Fidye yazılımının diğer sızma şekli ise hedef bilgisayarda bulunan bir yazılımın güvenlik açığından faydalanmaktır. Kullanıcıların sisteminde bulunan bazı güncel olmayan yazılımlar güvenlik açığı barındırabilmekte bu

durumdan faydalanarak da hedef sistemlere sızılabilmektedir [5].

Fidye yazılımları, değerli verileri kilitler ve çoğu zaman kırılmaz şifreleme algoritmalarıyla erişilmez hale getirir [6]. Hem şirketleri hem de ev kullanıcılarını hedef alan ve kârlı sonuçları nedeniyle son yıllarda yayılan bir siber tehdittir[7]. Bu yazılımları kullanan bilgisayar korsanları, dosyaları şifreledikten sonra tekrar verileri eski haline getirmek için kullanıcıdan fidye istemektedir. Bu fidye genellikle sanal para birimi olan Bitcoin olarak istenir. Fidye yazılımının fark edilen bir başka davranışı, sistemde nasıl çalıştırılacağı konusunda daha fazla talimat almak için bir komuta ve kontrol (C&C) sunucusuyla iletişim kurmaya çalışmasıdır. Ek dosyalar indirebilir veya dosyayı şifrelemek için gereken anahtarı transfer edebilmektedir [2].

Etkili bir güncelleştirme ve yama yönetimi stratejisinin günümüzdeki siber tehditlerin büyük bir yüzdesinin azaltılmasına yardımcı olduğu bilinmektedir. Sıfırıncı gün (Zero Day) güvenlik açıkları nispeten nadirdir, ancak etkileri daha yıkıcı olabilir. Bir yazılım üzerinde bulunan açık, yama yazılımı yayılıncaya kadar çalıştığı sistem üzerinde bir güvenlik açığı meydana getirmektedir. Sıfırıncı gün açık sayısı, 2015'te ortalama haftada bir ortaya çıkarken 2021'de günde bir ortaya çıkması ve uygulama saldırı yüzeyinin her yıl 111 milyar yeni kod satırı ile artması beklenmektedir [8].

Bazı raporlar, fidye yazılımlarını yalnızca finansal olarak motive olmuş suçluların bir aracı olarak değil, aynı zamanda bazı ülkelerin çıkarları için çalışan gruplar için de tanımlamaktadır. Ransomware, imalat, taşımacılık ve telekomünikasyon endüstrilerinden, finans şirketlerinden, kamu kurumlarından ve sağlık hizmetlerinden geniş bir yelpazedeki şirketleri etkilemektedir [7]. Saldırganlara ödenen paranın yanında, aynı zamanda ticari faaliyetlerin durmasına, şirketlerin kamu imajının sarsılmasına da neden olmaktadır.

Her ne kadar ekonomik etkileri ile ilgili raporlar kesin olmasa da, her yıl fidye yazılım suçları genişletilmiş çok uluslu etkilere neden olmaktadır. 2017'de WannaCry ve NotPetya saldırılarının küresel maliyetlerinin 8 milyar doların üzerinde olduğu tahmin edilmektedir. 2018'in ilk üç haftasında GrandCrab fidye yazılımı 50.000'den fazla sisteme bulaşmıştır. Fidye yazılımlarından sadece masaüstü sistemleri etkilenmemekte, aynı zamanda mobil fidye yazılımları da 2017'de etkisini artırmıştır. Antivirüs şirketleri, 2017 yılının ilk çeyreğinde bir önceki çeyreğe göre fidye yazılımı kurulum paketlerinde üç kat artış bildirmiştir [7]. Kötü amaçlı yazılım geliştiricileri, iyi niyetli bir program gibi

görünen kötü amaçlı yazılımların kullanıcılar tarafından bilgisayara indirilmesini ve yüklemesini sağlamaktadır.

İnternetin uçsuz bucaksız dünyası düşünüldüğünde ülkemizdeki herhangi bir sisteme misafir olan zararlı yazılım, sadece Türkiye'deki diğer bir sistem için değil dünyanın öbür ucundaki bir sistem için de risk oluşturabilmektedir. Bu nedenle zararlı yazılımlardan haberdar olmak, nasıl davrandıklarını ve ne yaptıklarını anlayarak gerekli önlemleri hızlıca almak, bu konudaki bilgi ve tecrübeyi paylaşmak çok önem arz etmektedir [9].

Fidye yazılımı bulaşma süreci aşağıdaki gibi özetlenebilir [1]:

E-posta tıklanarak, internetten dosya indirerek, herhangi bir güvenlik açığından faydalanarak zararlı yazılım bilgisayara aktarılır.

Bilgisayarda bulunan dosyalar şifrelenerek kullanım dışı bırakılır.

Kullanıcı-müşteri serbest bırakma notunu okur.

Paranın son teslimat tarihi ve Bitcoin hesabı verilir.

Kullanıcı-müşteri belirtilen süre içerisinde ödeme yapar.

Ödemenin yapılıp yapılmamasına göre bilgisayar kullanıma tekrar açılır veya tamamen kapatılır.

1.2. LİTERATÜR ARAŞTIRMASI

Zararlı yazılım analizine dair literatürde yapılan çalışmalar bulunmaktadır. [2]'de fidye yazılımı kodlayıcıları tarafından sergilenen tekniklere dayanarak, statik ve dinamik analiz tekniklerine dayalı bir model oluşturmuştur. Statik analiz için dosya sistemleri içerisine tuzak dosyalar yerleştirme ve kullanıcı sistemine gelen ve giden paketleri analiz etme yaklaşımlarında bulunmaktadır. Dinamik analiz için ağ paketi ayrıntıları derinlemesine analiz edilmektedir. Daha fazla hasarı önlemek için ağ paketi işaretlenmektedir ve ip adresleri güvenlik duvarına eklenmektedir.

[5]'te 3. Nesil Cerber fidye yazılım karakteristik davranış analizi için yapmış oldukları incelemeleri "Access Data Forensic Toolkit" yazılımı aracılığıyla gerçekleştirmiştir. Kayıt altına alınan veriler üzerinde network hareketleri Wireshark programı ile incelenmiştir. Yapılan incelemelerde tespit edilen ip adreslerinin whois (Alan Adı Sorgulama) kayıtları www.domaintools.com web adresi üzerinden ulaşılabilir olduğu

görülmüştür.

[6]'da saldırı sırasında sistem davranışları izlenerek analizi yapılmaktadır. Davranış analizi ile birlikte, sistemleri fidye yazılımı saldırısından korumak için SMBv1'in devre dışı bırakılması, perfc.dat ve psexec.dat adındaki dosyaların sysinternals üzerinden çalıştırılmasının engellenmesi önerilmektedir.

[10]'da Amoeba adı verilen otomatik yedeklemeyi destekleyen bir SSD yedekleme sistemi ile zararlı yazılımların önlenmesi önerilmektedir. Bu sistem, fidye yazılımı saldırılarını algılayabilen bir donanım hızlandırıcısı ve orijinal veri yedekleme için ek yükü en aza indirmek için bir yedekleme kontrol mekanizması ile donatılmıştır.

[11]'de fidye yazılımlarını algılamak amacıyla bir sınıflandırıcıyı eğitmek için en ayrımcı API çağrıları kullanılmaktadır. Yapılan çalışma ile çok sayıda fidye yazılım örneği analiz edilerek ayırt edici API çağrıları belirlenmiştir.

[12]'de zararlı yazılım analizlerinde kullanmak üzere analiz adımlarını gösteren bir model önerilmiş ve önerilen model ile web tabanlı zararlı yazılımının karakteristik davranış analizi için "Access Data Forensic Toolkit v6.2.1.10 (FTK)", "Process Explorer" "Cuckoo" araçları önerilmiştir.

[13]'te paket ve akış seviyelerini iki farklı bağımsız sınıflandırıcı olarak kullanan özel bir test ortamı oluşturarak ağ tabanlı saldığı tespit sistemi önerilmektedir.

[14]'te kötü amaçlı yazılımların tespitinde derin öğrenme yöntemlerini önermektedir. Fidye yazılımı yürütülebilir dosyalarının Windows ortamını hedef alan bir dizi veri kümesi kullanılmaktadır.

[15]'de gelişmiş fidye yazılım tehditlerini tespit etmek ve azaltmak için yazılım tanımlı ağ (SDN - Software-Defined Networking) kullanımını araştırmıştır. Yapılan araştırmaların kanıtlanması amacıyla WannaCry fidye yazılımı kullanılmıştır. Elde edilen sonuçlara dayanarak, bir SDN algılama ve azaltma çerçevesi tasarlanmış ve OpenFlow iletişim protokolüne dayalı bir çözüm geliştirilmiştir.

[16]'da fidye yazılımlarının adli analizi sürecinde yazılımsal ve fiziksel görüntü oluşturma yöntemlerini önermektedir.

[17]'de dijital adli analiz alanı araçlarının kötü amaçlı yazılımlar tarafından kullanılan şifreleme anahtarlarını bulmak ve fidye yazılımı saldırısının etkilerini azaltmak için kullanılıp kullanılamayacağını belirlemeye yönelik bir araştırma yapmıştır. Yapılan

çalışmada, adli analiz araçları ile fidye yazılımından etkilenen bir sistemden bellek bilgileri alınarak kullanılan simetrik şifreleme anahtarları tanımlanmaya çalışılmıştır.

[18]'de şifreleme aşamasından önce kripto-fidye yazılımını tespit edebilen Şifreleme Öncesi Algılama Algoritmasını (PEDA) önermiştir. PEDA iki seviye algılama sağlar; ilk algılama düzeyi, fidye yazılımı etkinleştirilmeden önce bilinen kripto-fidye yazılımı imzaları ile imza karşılaştırması yapılmasıdır. İmza, dosya içeriğinin hızlı ve doğru bir şekilde karşılaştırılmasını sağlayan SHA-256 (Güvenli Hashing Algoritması) kullanılarak oluşturulmaktadır. İkinci düzey algılama, şifreleme öncesi uygulama programı arabirimine (API) dayalı olarak kripto-fidye yazılımlarını algılayabilen Öğrenme Algoritmasının (LA) kullanılmasıdır.

[19]'da IoT bağlamında Ransomware'in evrimi, önlenmesi ve hafifletilmesi hakkında kapsamlı bir çalışma gerçekleştirmiştir. Bu çalışma IoT'deki Ransomware evrimi hakkında daha derin bilgiler vermektedir.

[20]'de bir yazılımın fidye yazılımı olup olmadığını belirlemek için süreç davranışı ve doğası arasındaki ilişkiyi araştırmaktadır. Buradaki amaç, bu yöntemi kullanmanın kötü niyetli yazılımlardan kaçınmaya yardım edip etmeyeceğini ve insan bağışıklık sistemini taklit eden makine öğrenimini kullanarak kendini savunma mekanizması olarak kullanılıp kullanılamayacağını görmektir.

[21]'de büyük bir kukla dosya oluşturarak bilgisayarları koruyan, bir saldırıyı tanımlayan ve önleyen bir çözüm önerilmektedir. Büyük bir kukla dosya, bir saldırgan tarafından şifrelenmek istenildiğinde bu işlem zaman almakta ve bu süreçte dosya sisteminin kalan içeriği kötü amaçlı yazılım tarafından erişilemez hale getirilmektedir. Önerilen mekanizma gerçek zamanlı bir ortamda test edilmiş ve faydalı olduğu kanıtlanmıştır.

[22]'de kötü niyetli eylemler için bellek işlemleri ve erişim kalıplarını incelemiş, bellek erişim görüntülerinin çıkarılmasına yönelik yeni bir yaklaşım sunmuştur.

[23]'de IoT (Nesnelerin İnterneti) cihazlarını kullanan ağlar için bir saldırı yüzeyi tanımlamıştır. Potansiyel riskleri azaltmak için güvenlik çözümlerinin sistematik olarak analiz edilmesini sağlayan bir tehdit modeli tanımlanmaktadır. Bir IoT mimarisi tasarlanarak bölgelere ayrılmış, sistemdeki güvenlik açıkları veya zayıflıkları ve bu alanı hedefleyebilecek saldırılar tanımlanmıştır.

1.3. TEZİN ORGANİZASYONU

Bu tez çalışmasının birinci bölümünde fidye yazılımları hakkında bilgi verilerek tezin kapsamına değinilmiş ve literatürde yer alan çalışmalar sıralanmıştır.

İkinci bölümde, fidye yazılımlarının tarihi, etkileme yöntemleri ve örnekleri ele alınmıştır.

Üçüncü bölümde fidye yazılım analizi için kullanılmak üzere hazırlanan Remnux ve Cuckoo SandBox deneysel ortamları hakkında bilgi verilmiştir.

Dördüncü bölümde, hazırlanan deneysel ortam kullanılarak gerçekleştirilen statik ve dinamik analizler üzerinde durulmuştur.

Beşinci bölümde, zararlı yazılım ve zararsız yazılım analizleri karşılaştırmalı olarak verilmiştir.

Altıncı ve son bölümde elde edilen bulgular değerlendirilerek gelecekte yapılması planlanan çalışmalara değinilmiştir.

2. FİDYE YAZILIMLARI

Bu bölümde fidye yazılımlarının gelişimi, çeşitleri ve fidye yazılımlarının detaylarına yer verilmiştir.

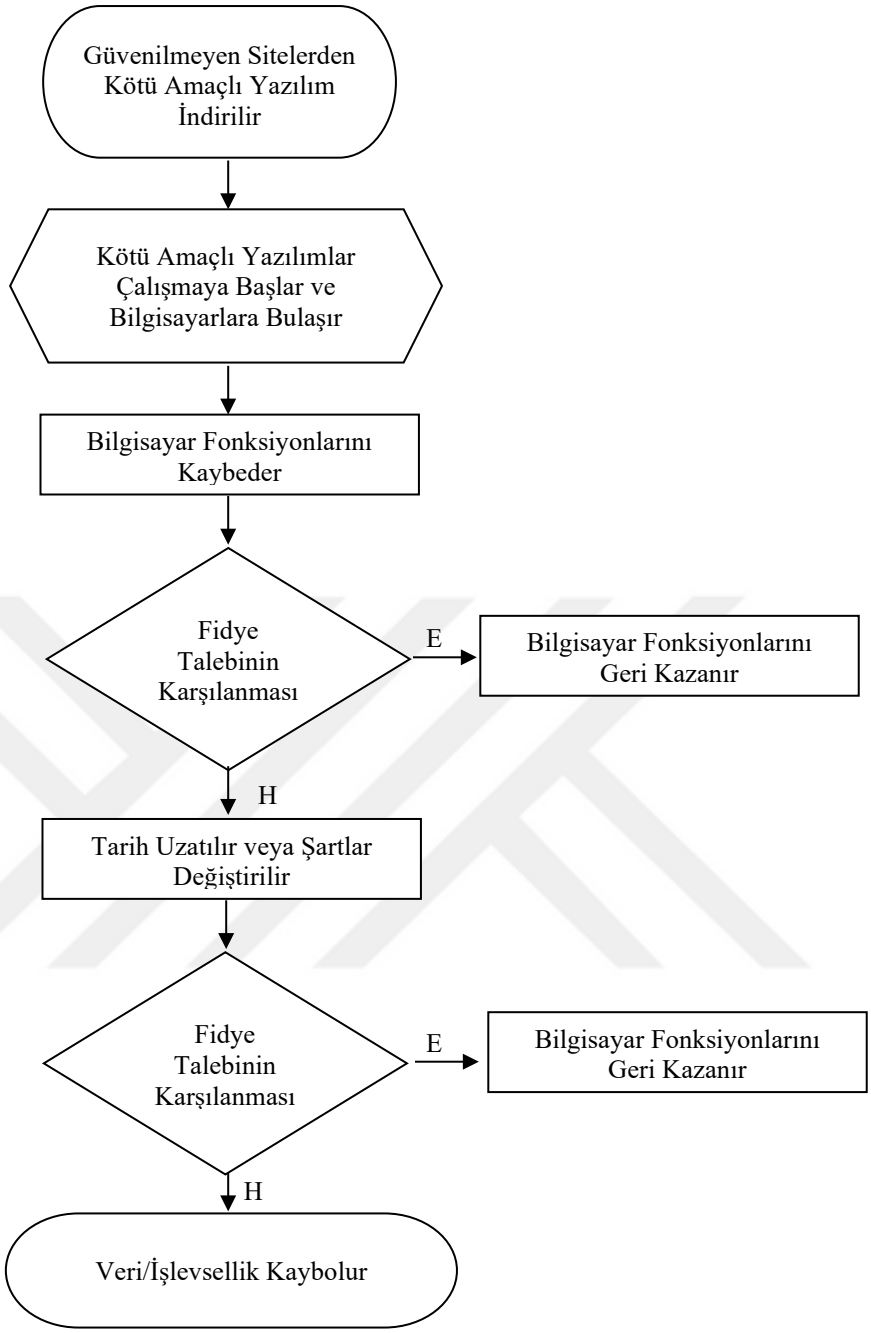
Ransomware saldırılarında diğer ülkelere göre en fazla etkilenen bölge %28 ile ABD'dir. Bunun yanında %16 ile Kanada, %11 ile Avustralya ve %9 ile Hindistan en çok etkilenen ülkelerdir. Etkilenen batı ülkelerinden bazıları %4 ile İtalya, %3 ile İngiltere, %2 ile Almanya, %2 ile Hollanda'dır. Bu istatistikler, siber suçluların temel olarak gelişmiş ülkeleri saldırılarına yönelik hedef aldıklarını göstermektedir [6].

Fidye yazılımı sistemi etkilediği ilk andan itibaren finansal zararlara neden olabileceğinden, fidye yazılımı saldırılarını azaltmak için etkili bir yol bulmak acil bir ihtiyaçtır. Örneğin Amerika'nın Atlanta eyaleti, 2018'deki son fidye yazılımı saldırısından kurtulmak için 2,6 milyon dolardan fazla harcama yapmak zorunda kalmıştır [10].

Zararlı yazılımın bulaştığı ağ içinde kalıcılığını sürdürmelerine ne kadar uzun süre izin verilirse, saldırılar ağ içinde diğer bilgisayarlara bulaşmak üzere hareket etme, hassas veri depoları bulma, daha fazla kurumsal ip adresi veya müşteri verilerine ulaşma çabası göstermektedir [24].

Fidye yazılımlarını tespit etmek zordur çünkü her ay yaklaşık 20.000 farklı çeşit ile ortaya çıkmaktadır. Fidye yazılımındaki her türlü değişikliği izlemek ve bunlara tepki vermek zaman alıcı ve yoğun emek isteyen bir iştir. Bu durumun üstesinden gelmek için uygun maliyetli ve etkili bir savunma önlemi gerekmektedir [25].

Zararlı yazılım analizleri için standart olarak uygulanan bir metot olmamakla beraber genel eğilim basitten karmaşığa doğru ilerlemektir. İlk olarak zararlı yazılım çalıştırılmadan elde edilebilecek tüm bilgilere ulaşmak daha sonra zararlı yazılımın kontrollü bir ortamda çalıştırılmasıyla davranış hareketlerini tespit etmek, son olarak ise zararlı yazılımın kod mimarisinin incelenmesi doğru bir yöntem olmaktadır [26]. Fidye yazılımının bilgisayar üzerinden çalışma yapısı Şekil 2.1'de yer almaktadır.



Şekil 2.1. Fidye yazılımını bilgisayar üzerinde çalışma yapısı.

Fidye yazılımı büyümesini etkileyen faktörler şöyledir [6]:

Şifreleme: Teknolojinin hızlı bir şekilde gelişmesiyle askeri, elektronik, banka sistemleri ve daha birçok yer kriptografi biliminin kullanım alanları haline gelmiştir. Günümüz sistemlerinde en önemli gereksinimlerden birisi bilgilerin sorunsuz bir şekilde taşınması ve gizliliktir. Verilerin güvenli bir şekilde yollanması ve karşı taraftan alınabilmesi için kriptografi bilimi aracılığıyla geliştirilen çeşitli şifreleme, anahtarlama ve çözümleme algoritmaları kullanılmaktadır. Kriptoloji algoritmalarından en yaygın kullanılanı ise

şifreleme algoritmalarıdır. Şifreleme algoritması şifrelenecek metni ve şifreleme anahtarını girdi olarak almaktadır. Çözümleme algoritması ise şifreleme algoritmasının tersi yönünde çalışmaktadır [27].

Etkili Bulaştırma Vektörü: Çoklu kullanıma açık olan serverlar, e-posta kullanımı, işletim sistemi ve programlar üzerinde bulunan açıklar saldırganların kurbanlara ulaşması için kolay yöntemler sunmaktadır. Fidye yazılımı grubu milyonlarca kullanıcının günlük olarak zararlı e-posta almalarına neden olan büyük spam kampanyaları oluşturmaktadır. Saldırganın önemli ölçüde kazanç sağlayabilmesi için çok fazla sayıda kullanıcıya virüs bulaştırması gerekmektedir [6].

Kripto Para Birimi: Para transferinin izlenmesinin zor olması sebebiyle kullanımı artmıştır. Saldırganların daha kolay para kazanmasını ve kendilerini güvende hissetmelerine sebep olmuştur. Fidye yazılımı ödemeleri sosyal ağlar kullanılarak yapılabilmektedir. Bununla birlikte, çoğu kripto para birimleri kullanılarak ödemeler gerçekleştirilmekte ve fidye yazılım ailelerinin %98'i Bitcoin kullanmaktadır [7].

RaaS (Ransomware as a Service): RaaS ile siber dünyaya yeni bir hizmet getirilmiştir. Altyapı olarak bulut hizmetleriyle aynı yapıdadır. Bu hizmet ile herhangi bir güvenlik açığı hakkında bilgisi olmayan veya kod yazmayı bilmeyen bir kullanıcı zararlı yazılım satın alarak bir saldırgana dönüşebilmektedir. Derin ağ üzerinde, bazı kötü niyetli bilgisayar korsanları insanlara fidye yazılımı satışı yapabilmektedir (Ransomware as a Service-RaaS); böylece kötü niyetli bir acemi kodlama bilgisi olmadan ve çok fazla çaba harcamadan bu zararlı yazılımları hızla yayabilir hale gelmektedir [2]. Derin ağ, internet'in çıktığı ilk tarihlerden itibaren arama motorları tarafından indekslenmeyen verilerin bulunduğu bilgileri içeren binlerce linkten oluşan bir sistemdir. Arama linki verilmeyen veya arama motorları tarafından bulunamayan bütün siteler derin ağa dahildir [28].

RaaS, yani hizmet olarak fidye yazılımı, her kullanıcının kurbanlara saldırmak için kendi özel fidye yazılımını kolayca alabileceği anlamına gelmektedir, böylece daha az beceri ve bilgiye sahip bir bilgisayar korsanının fidye yazılımını kullanması ve kurbanlarını takip etmek için bir kullanıcı ara yüzüne erişmesi mümkün olmuştur [6].

Saldırı grafikleri, büyük ve karmaşık bir ağı analiz etmek için en kolay ve iyi bilinen grafiklerdir. İnternet teknolojisindeki patlama ile birlikte çoğunlukla tüm ağlar risk altındadır. Ağın güvenliğini tehlikeye atmamak için ağın çalışması analiz edilir. Saldırı

grafiği, saldırganın bir ağdaki hedefine ulaşmak için izleyebileceği çeşitli saldırı yollarından oluşmakta, ağ yapılandırması ve güvenlik açıkları arasındaki ilişkiyi anlatmaktadır [6].

Exploit kitleri, kurbanın bilgisayarına kötü amaçlı yazılım yüklemek için güvenlik açıklarından yararlanmak amacıyla istemci makinelerde yazılım güvenlik açıklarını tarayan ve tanımlayan kötü amaçlı yazılım uygulamalarıdır. Exploit kitleri, saldırı altyapısının önemli bir parçasıdır ve fidye yazılımı da dahil olmak üzere sayısız tehdidi uygulamak için etkili bir yol sağlamaktadır [4].

Saldırı yollarından elde edilen bu yararlı bilgilerle, mevcut güvenlik açıklarının ağlarını korumaları için çeşitli önlemler alınabilir. Ağı analiz etmek için önce ağın Nessus güvenlik açığı tarayıcısı gibi bir tarama platformu ile taranması gerekmektedir.

Nessus, Tenable Network Security tarafından geliştirilen güvenlik açıklarını taramak için kullanılan bir tarama aracıdır. Nessus, sistemde güvenlik açığı olup olmadığını tespit eder ve korsanların ağa bağlı olan herhangi bir sisteme erişmek için kullanabilecekleri herhangi bir güvenlik açığını keşfederse alarm verir. Tarama, bilgisayarda 1200'den fazla kontrol çalıştırılarak, bu saldırıların herhangi birinin bilgisayara zorla girip girmeyeceğini görmek için test ederek gerçekleştirilmektedir [6].

Nessus tarafından her bir sistem için oluşturulan rapor, bu güvenlik açığı durumunun ciddiyet seviyesine bağlı olarak bu güvenlik açıklarını kategorilere ayırırken, o sistem için açık olanları da göstermektedir.

Fidye talepleriyle mücadele etmek amacıyla NoMoreRansom.org (“artık fidye yok” anlamına geliyor) adlı bir web sitesi bulunmaktadır. Intel Security, Interpol, Hollanda polisi ve Kaspersky Lab firmasının iş birliğiyle oluşturulan portal ücret ödemeden verilerin kurtarılabilmesi için yol göstermektedir. Bu işlem için bilgisayarda bulunan şifreli dosyalardan ikisi ve fidyecilerin notu sisteme yüklenerek yardım talebinde bulunulur. Sonrasında eğer mümkünse belgelere ulaşılabilir [29].

2.1. FİDYE YAZILIMLARININ TARİHİ

Şimdiye kadar kullanılan ilk fidye yazılımı, disket tarafından teslim edilen PC CYBORG/AIDS'tir ve 1989 yılında Joseph Popp tarafından yazılmıştır. Temel olarak sistemin yeniden başlatıldığı ve sistem numarası 90'a ulaştığında autoexec.bat dosyasının

yerini almaktadır, sistem kök dosyalarını şifrelemekte ve dizinleri gizlemektedir [30]. Bu fidye yazılımı, belirli sayıda yeniden başlatma işleminden sonra sabit disk içeriğini şifrelemektedir ve kullanıcıların şifre çözme anahtarını almak için bir ücret ödemesini istemektedir [2].

2005 yılında gasp fidye yazılımları ortaya çıkmıştır. Bilgiler geri alınmak istenildiğinde, saldırganlara fidye ödenmesini istemektedir. 2005'te saldırganlar kurbanın sistemini ihlal etmek için e-posta spamları gibi yeni yöntemler kullanmakta ve şifreleme için RSA kullanmaktadır [30].

2006 yılının ortalarında Gpcode, Troj.ransom.a, Archiveus, Krotten, Cryzip ve MayArchive zararlıları daha karmaşık RSA şifrelemeleri, her seferinde daha uzun anahtarlara sahip fidye şifreleme metotları kullanmaktadır [31].

2011 yılında bir fidye yazılımı, bilgisayarınızı kilitleyip Windows ürününün aktifleştirilmesi gerektiğini söyleyerek ödeme yapılmasını (fidye) istemektedir. Bu oldukça gerçekçi görünen bir zararlıdır.

2013 son 4 ayında 5 Milyon dolardan fazla fidye toplayan Stamp bazlı bir fidye yazılımı Mac OS sistemlerini hedef almıştır.

2015 yılından itibaren çoğu platformu etkileyen birçok fidye zararlısı çok büyük zararlara sebep olmaktadır [32].

Tripwire tarafından yapılan araştırmaya göre, Ransomware'in 2017 yılında kuruluşlara en fazla zarar verdiği, ardından DDoS, kötü amaçlı içerikler, kimlik avı ve bilinen/bilinmeyen güvenlik açıklarının geldiği belirtilmektedir [11].

2015 ve 2016 arasında, kötü niyetli olarak algılanan fidye yazılımı ailelerinin sayısında artış görülmektedir. Symantec'teki araştırmacılar, 2016 yılının ilk çeyreğinde günde ortalama 4.000'den fazla fidye yazılımı saldırısı gözlemlemektedir, bu da 2015 yılında gözlenen saldırılarda yüzde 300 artış olduğunu göstermektedir [13].

SonicWall'un 2017 yılındaki yıllık tehdit raporu, dördüncü çeyrek sonuna kadar saldırı sayısının 266,5 milyon denemeye kadar ulaştığını, 2016 yılında fidye yazılımı saldırı girişimlerinin sayısında on kat artış olduğunu belirtmektedir. Fidye yazılımı 2017 ve 2018'de en tehlikeli siber saldırılardan biri olmaya devam etmektedir [13].

Trend Micro tarafından fidye yazılımları 2018 için bir numaralı siber tehdit olarak adlandırılmaktadır. Buna göre, çoğu kuruluşun henüz yapmadıysa, bir aşamada fidye

yazılımı ile uğraşmak zorunda kalacağını varsaymak doğrudur. Veri kaybeden işletmelerin yaklaşık %90'ının iki yıl içinde kapanmaya zorlandığı göz önüne alındığında, fidye yazılımı saldırısına hazırlıksız olmak işletmelerin alabileceği bir risk değildir [24].

2.2. FİDYE YAZILIM TÜRLERİ

Dosyaları şifreleyen fidye yazılımları, kişisel dosya ve klasörleri şifreler, çoğunlukla belgeleri, resim ve videoları hedef alır. Bu yazılımlar şifreledikleri dosyaları disk üzerinden silmektedir. Kullanıcılar dosyalarına ulaşmak istediklerinde genelde dosyaların olması gereken yerde; dosyaları için ödeme yapmalarını isteyen bir metin belgesi bulmaktadır. Bazen metin belgesi yerine otomatik açılan bir pencere ile ödeme ayrıntıları ekrana yansıtılmaktadır.

Ekran kilitleyen fidye yazılımları (WinLocker), bu fidye yazılımları bilgisayar açıldığında ekranı kilitler ve tüm ekranı kaplar, ödeme yapılması istenilen bir uyarı gösterir. Kullanıcılar tarafından ekran kapatılamaz veya başka bir pencere açılamaz. Bu yazılımın farkı, kişisel dosyaların şifrelenmemiş olmasıdır.

MBR fidye yazılımları, Master Boot Record (MBR) bilgisayar açıldığında işletim sisteminin başlatılmasını sağlayan, hangi işletim sisteminin çalışacağını belirleyen sabit disk bölümüdür. MBR fidye yazılımları sabit diskin bu bölümünü değiştirerek normal başlatılma işlemini durdurmaktadır, erişim elde edebilmek için ödeme yapılması gerektiğini belirten bir parola ekranı gelmektedir.

Web uygulama fidye yazılımları, web sunucularını hedefleyen ve sunucudaki dosyaları şifreleyen fidye yazılımlarıdır. Bu zararlı yazılımlar genellikle içerik yönetim sistemlerindeki bilinen zafiyetlerden faydalanarak web sunucularına sızmaktadır ve web uygulamasının eski haline geri dönmesi için ödeme yapılmasını istemektedir.

Mobil cihaz fidye yazılımları, çoğunlukla Android işletim sistemli cihazlar olmak üzere mobil cihazlar da fidye yazılımlardan etkilenmektedir. Mobil cihazlara yüklenen sahte yazılımlar, uygulama marketleri yerine internetten indirilen uygulamalar, beraberinde fidye yazılımları getirebilmektedir. Bu fidye yazılımları mobil cihazlarda bulunabilecek zafiyetlerden faydalanarak cihazı şifrelemektedir ve dosyalara erişim için belli bir süre içinde ödeme yapılmasını istemektedir.

Son yıllarda akıllı mobil cihazlar yaygın olarak tercih edilmektedir. En popüler mobil

işletim sistemi olan Android, %85,9'luk küresel payla pazara hakim durumdadır. Android işletim sisteminin açık yapısı ve kullanıma hazır uygulama dağıtım mekanizması birçok saldırganı cezbetmektedir. Android işletim sistemli cihazlar kazançlı hedefler haline gelmekte ve fidye yazılımlarının yayılması için ideal ana makineler haline gelmektedir [33].

Kripto fidye yazılımı, kullanılan şifreleme sistemine dayalı olarak üç türe ayrılır [13]:

Simetrik Şifreleme Sistemli Fidye Yazılımı: Şifreleme ve şifre çözme için aynı anahtarı kullanarak kurbanın dosyalarını şifrelemek için simetrik bir şifreleme algoritması kullanılır. Bu, kurbanın ters mühendislik veya bellek tarama teknikleri uygulayarak gizli anahtarı kurtarmasını makul hale getirmektedir.

Asimetrik Şifreleme Sistemli Fidye Yazılımı: Bu türde, fidye yazılımı dosyasına gömülü olan veya komuta ve kontrol (C&C) sunucusuyla iletişim sırasında indirilen bir ortak anahtar, kurbanın dosyasını şifrelemek için kullanılmaktadır.

Özel anahtar sadece saldırganla birlikte saklandığından, kurbanın fidye ödemeden onu alması imkansızdır. Ancak, bu teknik dosyaları şifrelerken daha fazla kaynak tüketmektedir.

Hibrit Şifrelemeli Fidye Yazılımı: Bu türde, kurbanın dosyalarını şifrelemek için dinamik olarak oluşturulmuş bir simetrik anahtar ve bellekten temizlendikten sonra simetrik anahtarı şifrelemek için önceden yüklenmiş bir ortak anahtar kullanılmaktadır.

Çoğu modern kripto fidye yazılımı ailesi bu tekniği her iki şifreleme türünden de yararlanmak için kullanmaktadır.

En yaygın fidye yazılımı türleri, hem simetrik hem de ortak anahtar tabanlı şifreleme düzenleri de dahil olan bir şifreleme türü kullanmaktadır. Ortak anahtar şifrelemesine dayanan fidye yazılımları, şifreleme anahtarları bir uzaktan komuta ve kontrol (C&C) sunucusunda saklandığından, etkisinin hafifletilmesi özellikle zordur.

Fidye ödenmesi için genellikle bir zaman sınırı vardır, kullanıcılara kripto para birimi (ör. Bitcoin) satın almak için özel bir web sitesi ve fidye ödeme konusunda adım adım talimatlar verilmektedir [34].

2.3. EN ETKİLİ FİDYE YAZILIMLARI

Birçok fidye yazılımı vardır, bu yazılımlardan vermiş olduğu maddi zararlar açısından en tehlikeli olarak belirtilenler aşağıdaki gibi listelenir [1]:

2.3.1. GoldenEye

Bu fidye yazılımı ve saldırısı Ukrayna'da rapor edilmiştir. Diğer fidye yazılımlarına benzer şekilde dosyalara zarar vermektedir, tüm bilgisayar sistemini hedef almaktadır. Sistemdeki dosyaları erişilemez hale getiren bazı ana dosya tablosunu kullanmaktadır. Bu zararlı yazılım kurbanların neredeyse 9,000 ABD dolarına mal olmaktadır.

2.3.2. WannaCry

Bu yazılım, en tehlikeli ve en kötü fidye yazılımı türlerinden biridir. Tüm dünyada 200.000'den fazla sisteme yayılmıştır. Bu saldırı temel olarak, işletim sistemi güncellemelerinin yok sayıldığında aktif hale gelmektedir. Dünyadaki zarar maliyeti, 2015'te 35 Milyar $, 2017'de 5 Milyar $ olarak tahmin edilmiştir.

2.3.3. Cryptolocker

Bu zararlı yazılım sistemde çalıştığı takdir de birkaç dakika içerisinde bütün verileri güçlü bir algoritma ile şifrelemektedir. Verilerin şifrelenme işlemi bittikten sonra kurban kullanıcının karşısına bir pencere çıkarır ve bu pencerede para ödeme isteği bilgileri yer alır. Eğer belirtilen miktarda para ödemesi yapılmadığı durumda verilerin şifreleri açılmaz ve veriler kurtarılamaz. Ücreti ödeme sistemi Bitcoin para birimi ile gerçekleştirilmektedir. Bu sayede alıcılar asla yakalanamamaktadır. Maliyetinin yaklaşık 300 milyon dolar olduğu belirtilmektedir [1].

2.3.4. Locky

Sisteme girer girmez dosyaları AES-128 şifrelemesi ile kilitlemektedir. Bu şifreleme işlemi bittiğinde kurban dosyalarına ulaşamaz hale gelir. Bu dosyaları geri getirmenin tek yolu kod çözücüyü almaktır ve bu araç Locky virüsü yazılımcılarındadır. Dosyaları kilitlenen kullanıcılardan yaklaşık 400$ fidye ödemesi istenilmektedir. Böylece kişisel dosyalarını deşifre edecek kodun kullanıcılara verileceği söylenir. Ancak güvenlik uzmanları kurbanların bu fidyeyi ödememesini önermektedir. Çünkü dosyalarınızın geri geleceğinin garantisi yoktur.

2.3.5. Petya

WannaCry gibi Windows SMBv1 güvenlik açığı (MS17-010) sayesinde hızla yaygınlık göstermiştir. NSA'in ShadowBrokers tarafından açığa çıkarılan exploitlerinden olan EternalBlue'yu kullanarak sisteme sızmaktadır ve sonrasında WMIC ve PSEXEC kullanarak ağda yayılma yeteneğine sahip olmaktadır. SMBv1 güvenlik açığının dışında diğer yayılma şekli ise spam e-postalardır. Kullanıcılara CVE-2017-0199 açığını kullanmak koşulu ile yayılmaktadır. Petya saldırısında, fidye notu, bireysel şifre çözme anahtarlarını almak için kurbanlardan Bitcoin cinsinden 300 ABD Doları ödenmesini talep eder. Çoğunlukla bu saldırı Avrupa'ya yayılmakta ve Brezilya, Almanya, Rusya, Hindistan ve ABD dahil olmak üzere 64 ülkede daha gözlenmektedir [30].

2.3.6. Powerware

Bu fidye yazılımı güvenlik firması Carbon Black tarafından gözlemlenmiştir. Bu, Microsoft Word ve PowerShell komut dosyası arabirimini kullanarak işletmeleri hedeflediği için diğerleri arasında oldukça ilginç bir yer almaktadır.

2.3.7. zCrypt

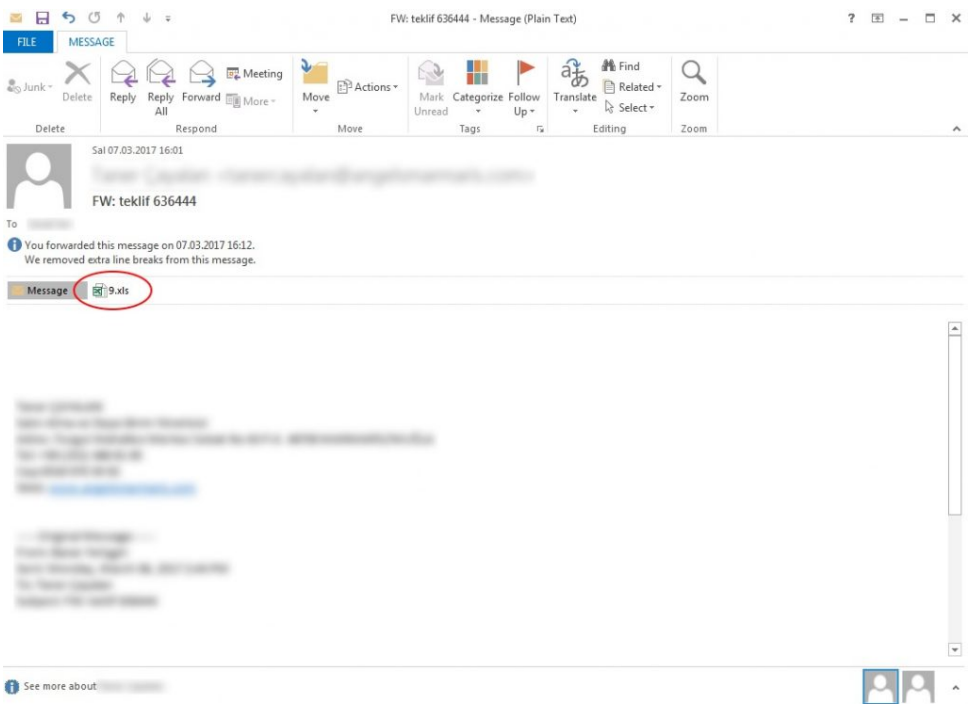
Bu tür fidye yazılımı, yaygın olmayan bir yöntem üzerine odaklanır. Kurban sistem bulmak için kötü amaçlı e-postalara bağlı değildir ve USB belleklerle yayılabilir. Diğer fidye yazılımları gibi tüm dosyalara saldırmak yerine, sadece değiştirilebilecek ve zarar verilebilecek önemli dizinleri bulmaktadır.

2.4. KULLANICILARA GÖNDERİLEN FİDYE YAZILIMI ÖRNEKLERİ

Bu bölümde kullanıcıların karşılaşabilecekleri fidye yazılımı örneklerinden bahsedilmektedir.

2.4.1. Örnek 1: Fiyat Teklif E-Postaları

Oltalama saldırısı ile hedeflere iletilen örnek e-posta içeriği Şekil 2.2'de yer almaktadır. Saldırgan, hedeflere fiyat teklifi içerikli mail atarak sosyal mühendislik gerçekleştirmektedir. Bu maillerde kimi zaman zararlı Office / JS dosyaları eklenmiş olarak bulunurken, kimi zaman ise dropbox linki üzerinden paylaşılmaktadır [35].

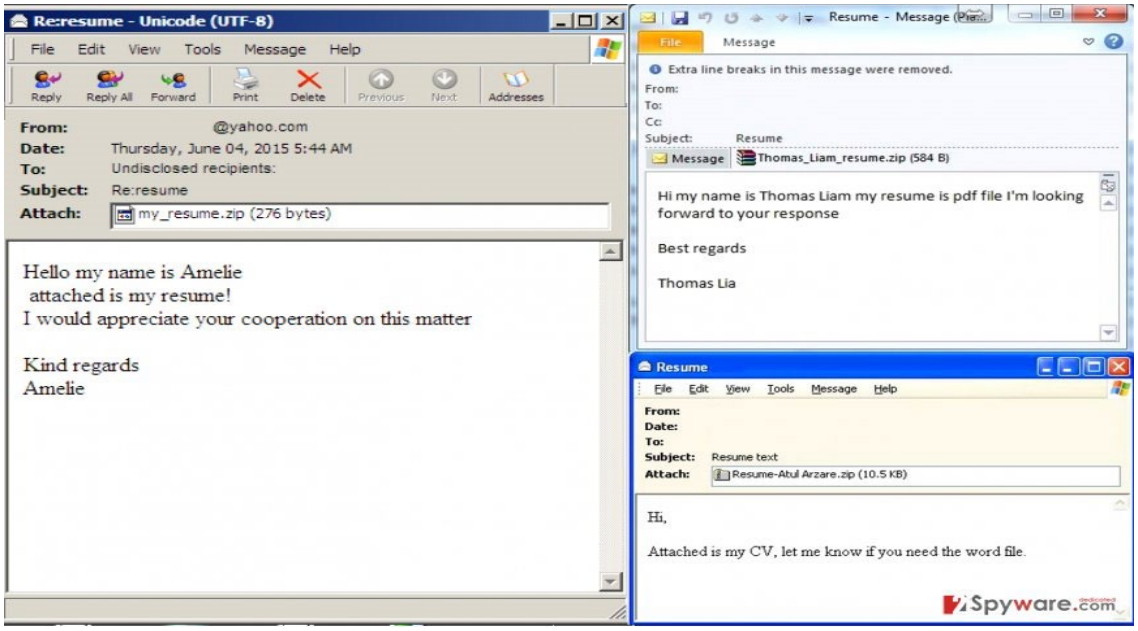


Şekil 2.2. Fiyat teklif e-posta örneği.

2.4.2. Örnek 2: Özgeçmiş veya İş Başvurusu Yapan E-Postalar

Şekil 2.3'deki gibi ekli bir özgeçmiş içeren kimlik avı e-postaları genellikle işe alım uzmanlarına, yöneticilere veya işe alma kararları veren şirket sahiplerine gönderilmektedir. Bu tür e-postalar genellikle alıcıyı ekli özgeçmişi açmaya davet eden yalnızca birkaç satır metin içermektedir.

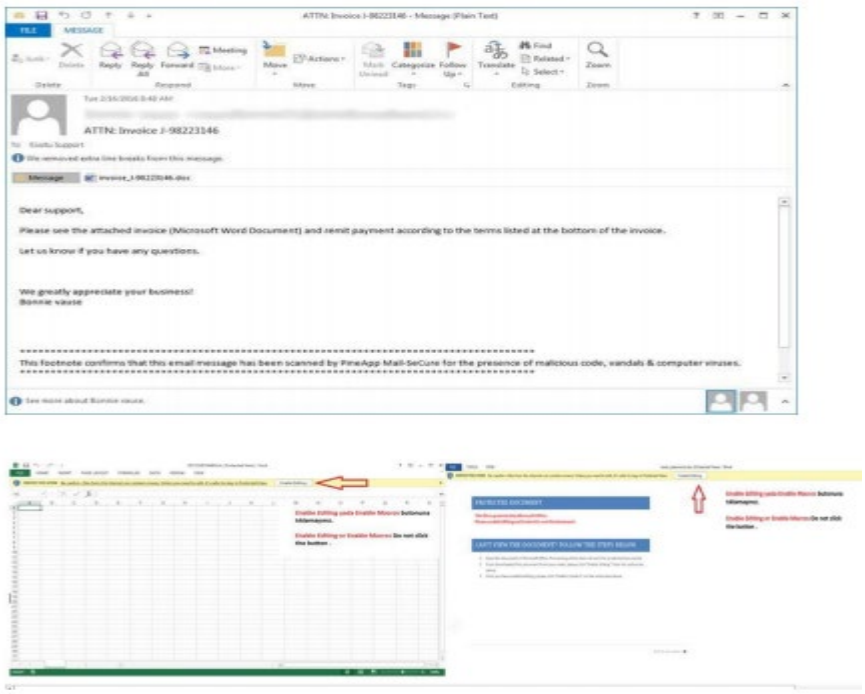
Genellikle, dolandırıcıların belirli bir şirkete veya sağlık kuruluşuna bulaşmaya çalışırken bu kimlik avı e-postalarının ikna edici olmasını beklemektedir. Bu tür fidye yazılımı e-posta örnekleri çoğunlukla CryptoWall 3.0, GoldenEye ve Cerber spam kampanyalarında kullanılmıştır [36].



Şekil 2.3. İş başvurusu için özgeçmiş e-posta örneği.

2.4.3. Örnek 3: Locky Fidye Yazılımı Oltalama E-Postası

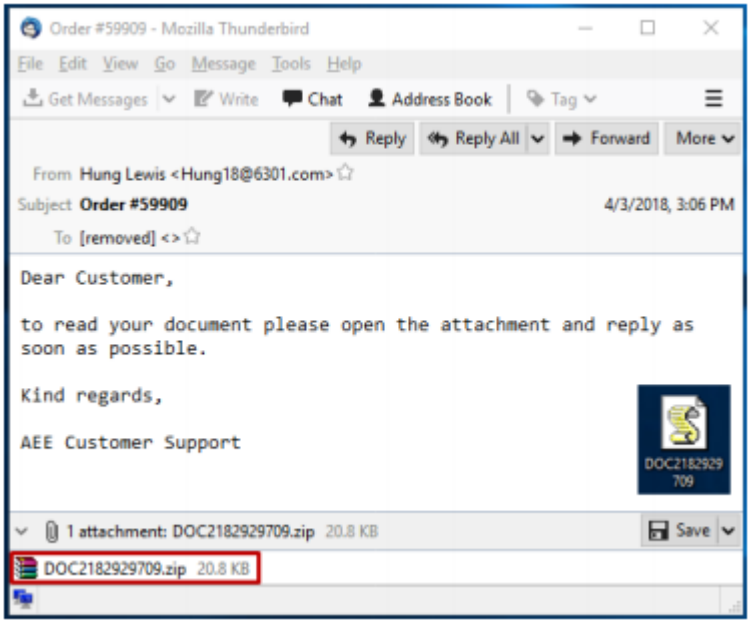
Örneği Şekil 2.4'de gösterilen bir mail ile gönderilen dosya eki Excel formatındadır ve açıldığında düzenlemenin etkinleştirilmesini veya makroların etkinleştirilmesini istemektedir. Bu işlem yapıldığında sistem ele geçirilir, fidye ödemeye zorlayacak biçimde tüm dosyaların şifrelenmesine sebep olmaktadır.



Şekil 2.4. Locky fidye yazılımı e-posta örneği.

2.4.4. Örnek 4: GrandCrab Yayılma Mekanizması

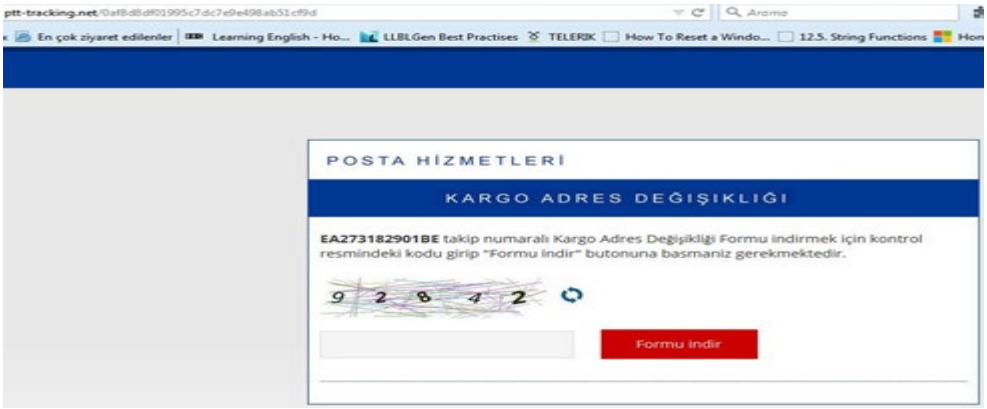
GrandCrab zararlısına ait ilk versiyonların RIG ve GrandSoft exploit kitleri ile spam mailler aracılığıyla dağıtılmak için kullanıldığı görülmüştür. Bir örneği Şekil 2.5'te yer verilen spam maillerin içerisinde ek olarak yerleştirilmiş ZIP uzantılı dosyaların yer aldığı görülmüş ve zip içerisinde yer alan javascript dosyasının çalıştırılarak GrandCrab zararlısına ait payload dosyasının indirilerek sisteme enfekte olduğu tespit edilmiştir.



Şekil 2.5. GrandCrab fidye yazılımı e-posta örneği.

2.4.5. Örnek 5: Kargo Takip Uygulaması

Şekil 2.6'de gösterildiği gibi kargo takip sisteminin bir benzerini klonlayan sanal hırsızlar form indirme seçeneği ile zararlı yazılımın indirilmesini sağlamak üzere bir yöntem takip edebilmektedir [37].



Şekil 2.6. Kargo takip ile oltalama e-posta örneği.

2.4.6. Örnek 6: Fatura E-Postaları

Şekil 2.7'deki gibi gönderilen fatura üzerinde yer alan "Faturanızı hemen ödemek için tıklayın" ve "Faturanızla ilgili detaylı bilgi" butonları kullanıcıları doğrudan zararlı bir web sayfasına yönlendirebilmektedir [38].



Şekil 2.7. Fatura ile oltalama e-posta örneği.

2.5. ANALİZ YÖNTEMLERİ

Analiz işleminde kullanılacak yöntemler temel olarak statik analiz ve dinamik analiz olmak üzere ikiye ayrılmaktadır.

Statik analiz, kötü niyetli yazılımı çalıştırmadan yapılan analiz yöntemlerini kapsar. Basit statik analiz ve ileri statik analiz olarak ikiye ayrılır.

Basit statik analiz: Dosya formatının tespiti, derinlemesine kod analizi yapılmadan kelimelerin incelenmesi, analiz edilecek zararlının anti virüsler karşısındaki tepkisinin ölçülmesi, hash değerinin alınmış halinin daha önceki hashler ile karşılaştırılması, uygulamanın packed ya da obfuscated edilmiş olup olmadığının programlar yardımıyla tespit edildiği bölümdür. Zararlı yazılımın statik analizine geçildiğinde karşılaşılan ilk terimler pack ve obfuscate terimleridir. Pack, analiz işlemini engellemek amacıyla kullanılan bir yöntemdir. Yazılımın gerçek kodu sıkıştırılır, çözmek için kullanılan bir anahtar ile çalıştırıldığında hafıza içerisinde çözülür. Obfuscate, yazılım kodlarının anlaşılmasının zorlaştırılması için kullanılan yöntemdir. Örneğin kod içerisindeki isim değişkeni ser2a4c şeklinde görüntülenirse bu değişkenin isim alanını tuttuğunun anlaşılması zorlaşmaktadır.

İleri statik analiz: Zararlı yazılımın işleyişini öğrenmek amacıyla düşük seviye programlama dillerine dönüştürülerek, içerisinde geçen kelimelerin, bağlantılı

kütüphaneler ve fonksiyonlar gibi özelliklerinin analiz edilmesidir.

Statik analizde kullanılan temel yazılımlar aşağıdaki gibidir:

Portable Executable : Taşınabilir ve çalıştırılabilir dosyalardır. Buna uzantısı .exe vb. olan dosyalarda denilebilir.

Packer: Bir yazılımı sıkıştırmaya yarayan yazılımdır.

Unpacker: Sıkıştırılmış kodu eski haline getirmek için kullanılan yazılımdır.

PE Sections: Çalıştırılabilir dosyamızın içerdiği Code, Data gibi bilgileri tutan bölümlerdir.

Peid: Zararlı yazılımın, hangi yazılım kullanılarak pack edildiğini bulmak için kullanılan yazılımdır.

Disassembler: İşlemcinin anlayabildiği makine kodunun insanların anlayabileceği şekilde okunabilir hale getiren yazılımlardır.

Decompiling: Paketlenerek kullanıma hazır hale getirilmiş bir programın kaynak kodlarına erişilebilir hale getirilmesini sağlayan yazılımlardır.

Dinamik analiz, oluşturulmuş bir laboratuvar ortamında zararlı yazılımın çalıştırılarak, sistem üzerinde yaptığı değişikliklerin incelenerek analiz edilmesidir. Yazılım dinamik analiz için çalıştırıldığında sistemi bozabilir, çalıştığı diski silebilir, başka sistemleri etkileyebilir, internet üzerinden bir sisteme saldırı düzenleyebilir. Bu nedenle yalıtılmış bir ortamda çalıştırılması gerekir. Dinamik analiz, zararlı yazılımın hareket kabiliyetini ve kapasitesini tam olarak görebilme imkanı sağlamaktadır [12].

Basit ve ileri dinamik analiz olmak üzere ikiye ayrılır.

Basit dinamik analiz: Çalıştırılan uygulamanın davranışsal analizinin yapıldığı kısımdır. Uygulamanın ağ üzerindeki davranışların, dosya ve kayıt defteri üzerinde yaptığı değişikliklerin, oluşturulan işlem süreçlerinin incelendiği kısımdır.

İleri dinamik analiz: Zararlı yazılımın çalıştırılırken debug edilmesi işlemidir. Bu aşamada işlemci komutları, registerlar üzerindeki değişimler, bellek dökümü, bellek alanının incelenmesi, fonksiyon çağrıları izleme gibi işlemler yapılmaktadır.

Regshot: Analiz edilecek yazılım çalıştırılmadan önce ve çalıştırıldıktan sonraki kayıt defteri aktivitelerini kıyaslayarak oluşan farklılıkları metin belgesi halinde ya da ".html" olarak aktarılmasını sağlamaktadır.

Process monitör: Dinamik analiz sırasında oluşturulan dosyaların, ağ aktivitelerinin ve kayıt defterinin gözlemlenmesini sağlamaktadır. İçerisinde birçok filtre barındırır. Göstermiş olduğu dosya ve kayıt defteri aktiviteleri ile dinamik analiz aşamasında önemli bilgiler sağlamaktadır.

Wireshark: Bilgisayara ulaşan paketleri yakalamaya ve bu paketlerin içeriğini görüntülemeye imkan tanır. Bilgisayara bağlı olan her türlü ağ kartlarındaki (Ethernet kartı veya modem kartları) tüm TCP/IP mesajlarını analiz edebilen bir programdır. Wireshark, günümüzde çok amaçlı kullanılmaktadır. Şebeke problemlerinde sorun çözmek, güvenlik problemlerini sınamak, uygulamaya konulan protokollerde oluşan hataları onarmak veya arındırmak, ağ protokolünün içerisindeki bilgileri öğrenebilmek için Wireshark programı kullanılır. Analiz edilen yazılımın çalışmasının ardından HTTP, DNS, TCP, UDP gibi protokol aktivitelerini kaydederek araştırmacılara önemli veriler sağlamaktadır.

Analiz İşlemini Zorlaştırmak İçin Kullanılan Yöntemler [39]:

Anti Debugging: Debugging işleminin zorlaştırılması/engellenmesi sağlanır.

Anti Disassembler: Disassembler yanıltılarak, kodun yorumlanması, analiz edilmesi zorlaştırılır/engellenir.

Anti VM: Programın sanal makinede çalışıp çalışmadığı tespit edilir.

Gizleme (Obfuscation): Byte kodların kaynak koduna çevrilmesi ve analiz edilmesi zorlaştırılır/engellenir.

Paketleme: Statik kod analizini zorlaştırma adına zararlı yazılımın sıkıştırılmasıdır.

3. DENEYSEL ANALİZ ORTAMI HAZIRLAMA

Bu bölümde yazılımların deneysel analizinin yapılması amacıyla çalışma ortamının kurulum aşamaları detaylı olarak bahsedilmektedir.

Analiz ortamının kurulumunun yapılacağı işletim sistemi olarak Ubuntu 16.04 dağıtımı kullanılmaktadır. Kurulum yapılan bilgisayar I5 8265 işlemci, 8 GB ram bellek, 2 GB ekran kartı, 256 GB SSD disk donanımlarına sahiptir.

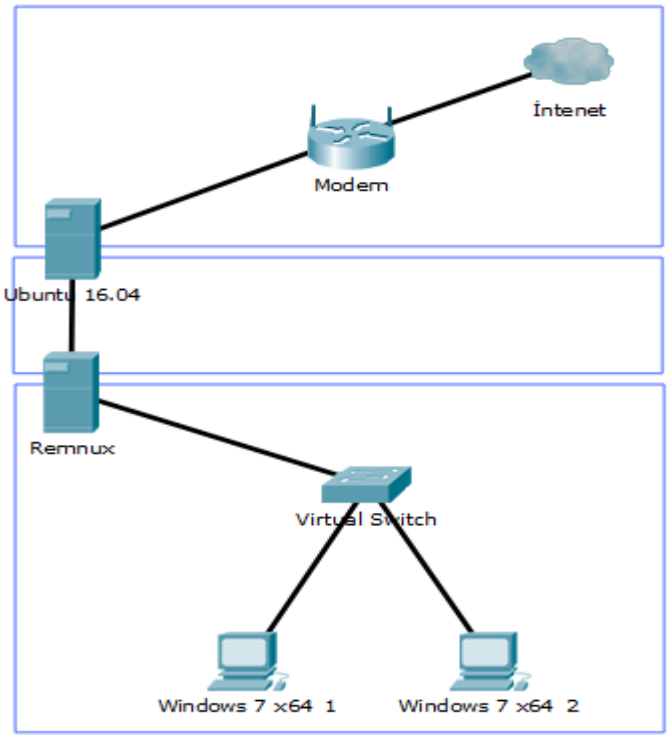
3.1. REMNUX ANALİZ ORTAMININ HAZIRLANMASI

Remnux, kötü amaçlı yazılımlar üzerinde tersine mühendislik ve analiz işlemlerinde kullanılan Linux araç setidir. Ubuntu tabanlı Linux dağıtımıdır. Adını da amacını ifade eden İngilizce kelimelerin kısaltılmasından almaktadır (Reverse-Engineering Malware Linux). İlk sürümü 2010 yılında yayımlanan Remnux, David Westcott'un kapsamlı yardımlarıyla Lenny Zeltser tarafından geliştirilmektedir. Zararlı yazılım analizi yapmak isteyen herkesin özgürce kullanabileceği bir yazılımdır. Analiz amacıyla bulunması, ulaşılması, kurulması ve yapılandırılması zor olabilecek çeşitli araçların kullanımını daha kolay bir hale getirmeyi ve zararlı yazılım analizi yapan kişileri sadece temel amaçlarına yönlendirmeyi hedeflemektedir.

Windows ve Linux kötü amaçlı yazılımlarını analiz etmek, gizlenmiş JavaScript gibi tarayıcı tabanlı tehditleri incelemek, şüpheli belge dosyalarını keşfetmek için birçok araç içermektedir. Davranışsal kötü amaçlı yazılım analizi yaparken izole bir laboratuvardaki şüpheli ağ trafiğini kesmek için kullanılmaktadır.

Remnux dağıtımı ile birlikte gelen varsayılan kullanıcı adı "remnux", şifresi ise "malware"dir. Zararlı yazılım analizinde Remnux üzerindeki hangi araçların ve özelliklerinin kullanılacağını bilmek etkili bir analiz için önemli kavramlardan biridir [9]. Kullanılan dağıtım Ubuntu 14.04 altyapısı üzerinde çalışan remnux-6.0-ova-public.ova dağıtımıdır. Birçok dağıtımda olduğu gibi temel kullanıcı işlemlerini yerine getirmek için kullanılan programların yanında https://remnux.org/docs/distro/tools/ adresi üzerinden kullanılabilir tüm araç listesine ulaşılmaktadır.

Remnux analiz ortamı kurulum, Şekil 3.1'de gösterilen topoloji ve Çizelge 3.1'de yer alan ip adres bilgilerine göre ağ yapılandırılması gerçekleştirilmektedir. Bu bilgilere uygun olarak Ubuntu 16.04 kurulu fiziksel bilgisayar üzerine Remnux sanal bilgisayarı ve Windows istemci sanal bilgisayarları kurulumu yapılmaktadır.



Şekil 3.1. Remnux analiz ortamı topolojisi.

Çizelge 3.1. Remnux analiz ortamı ip adres bilgileri.

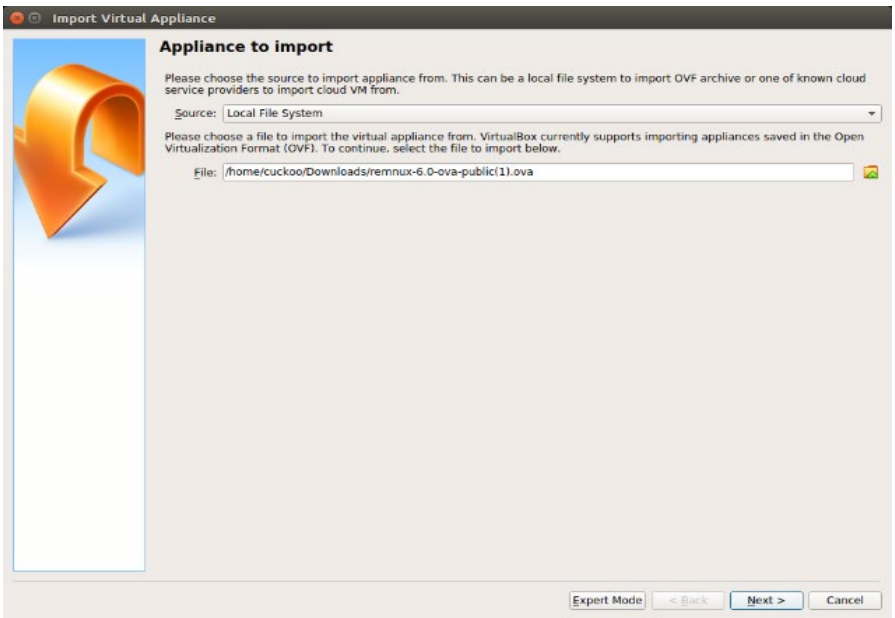
Bilgisayar Türü	Fiziksel Bilgisayar		Sanal Bilgisayar		Sanal Bilgisayar 1	Sanal Bilgisayar 2
İşletim Sistemi	Ubuntu 16.04		Remnux		Windows7 x64	Windows7 x64
Ethernet Adı	wlp2s0	vboxnet1	eth0 (Host-Only)	eth1 (NAT)		
Ip Adresi	192.168.2.99	192.168.10.1	192.168.10.10	10.0.2.15	192.168.10.20	192.168.10.30
Alt Ağ Maskesi	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Varsayılan Ağ Geçidi	192.168.2.1				192.168.10.10	192.168.10.10
DNS	195.175.39.39				195.175.39.39	195.175.39.39

1- Kurulum işlemi Şekil 3.2'de sürüm bilgisi verilen "ORACLE VM Virtualbox 6.1" sanallaştırma yazılımı üzerine yapılmaktadır. Bu nedenle öncelikle işletim sistemi üzerinde Virtualbox 6.1 kurulu durumda olmalıdır.



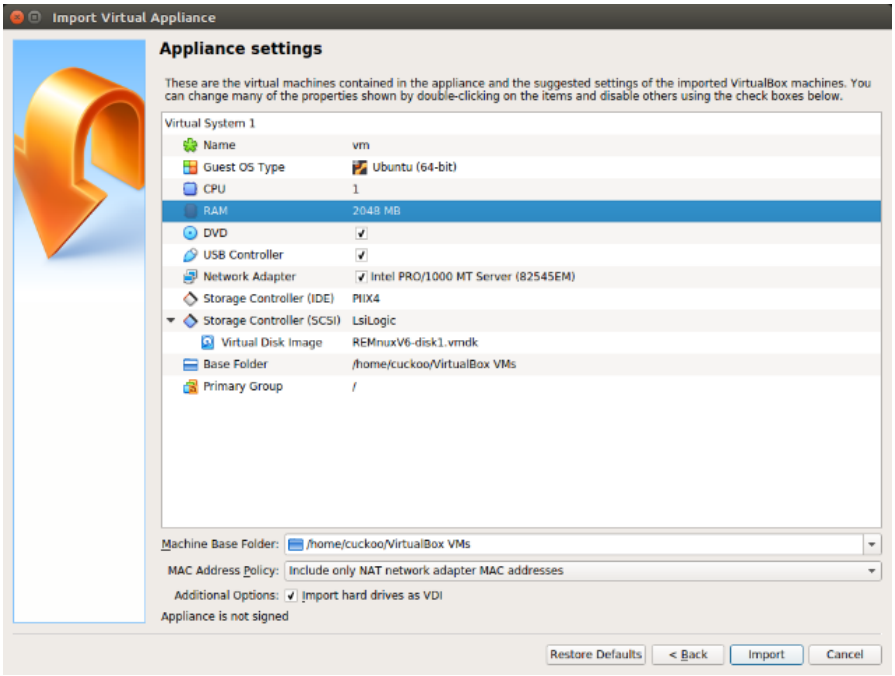
Şekil 3.2. Virtualbox sürüm bilgisi.

2- Virtualbox çalıştırılarak "File – Import Appliance" menü seçeneği ile Remnux resmi web sitesinden indirilen ova uzantılı imaj dosyasının seçilmesi işlemi Şekil 3.3'te gösterilmektedir.



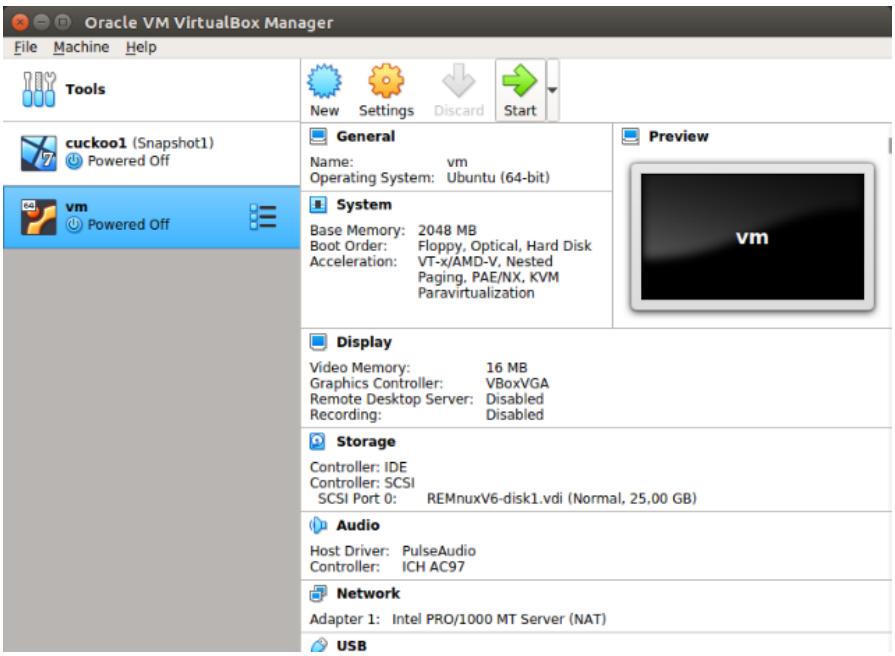
Şekil 3.3. Remnux ova dosyasının import edilmesi.

3- Ram bellek değerinin 2048 MB yapılması ve diğer temel ayarlara Şekil 3.4'de yer verilmektedir.



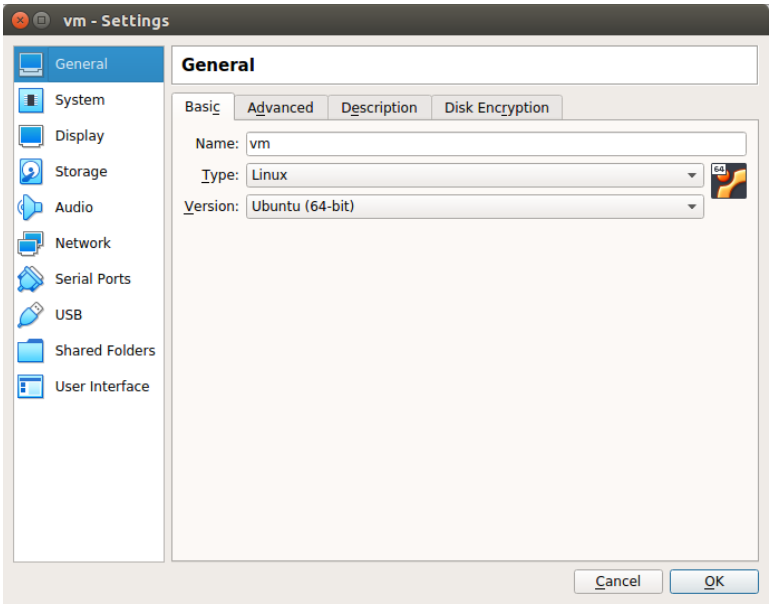
Şekil 3.4. Remnux ram bellek gösterimi.

4- Import seçeneği seçilmesi ile sanal bilgisayar oluşturulmaktadır. Şekil 3.5'de sanal bilgisayarın temel görünümü verilmektedir.



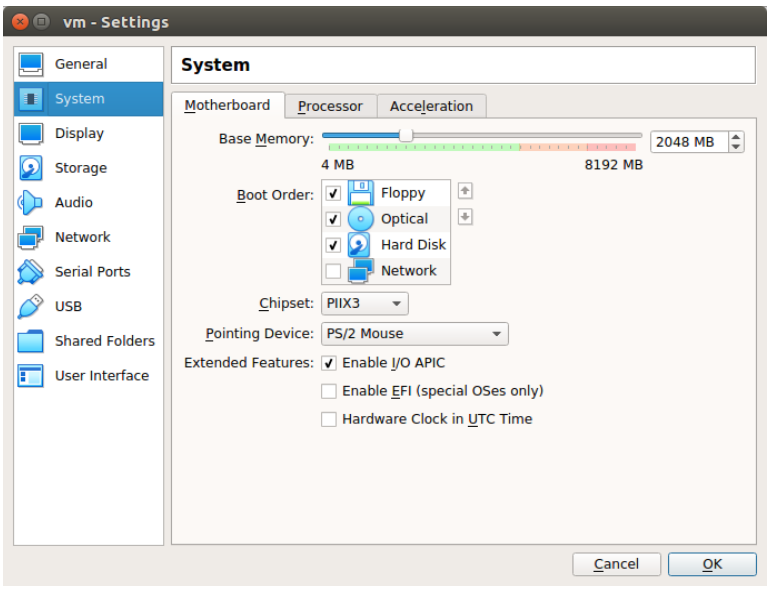
Şekil 3.5. Remnux sanal bilgisayar temel görünümü.

5- “Machine – Settings” seçeneği ile isteğe bağlı ayarlar yapılır. Şekil 3.6’da görüldüğü gibi genel ayarlar penceresinde işletim sistemi versiyonu, tür, isim gibi bilgilerin yanında anlık görüntü klasörü, sürükle bırak ayarları, açıklama ve disk şifreleme işlemi ayarları yapılmaktadır.



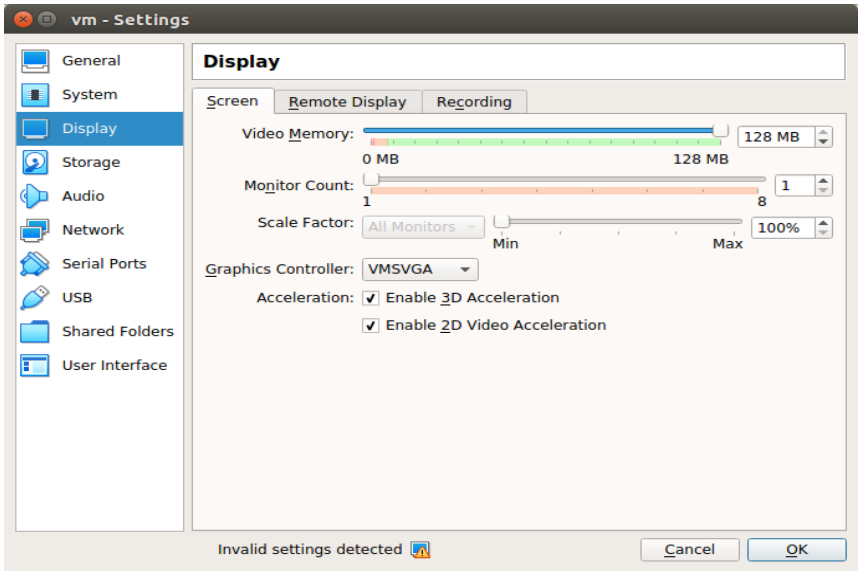
Şekil 3.6. Remnux genel bilgi penceresi.

6- Şekil 3.7’de görüldüğü gibi temel sistem ayarları penceresinde ram bellek, önyükleme sırası, chipset seçimi, işlemci kullanımı oranı ayarı ve sanallaştırma ayarları yapılmaktadır.



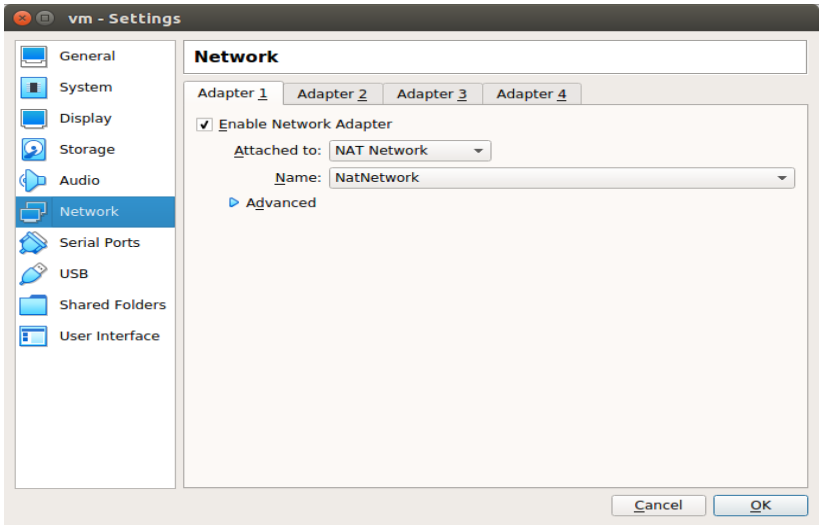
Şekil 3.7. Remnux sistem penceresi temel ayarları.

7- Şekil 3.8'de görüldüğü gibi ekran ayarları penceresinden ekran kartı temel ayarları yapılmaktadır. Bu pencerede ekran kartı performansını artırmak amacıyla Video Memory 16 MB'tan 128 MB'a çıkarılır, "Enable 3D Acceleration" ve "Enable 2D Video Acceleration" seçenekleri etkinleştirilir.

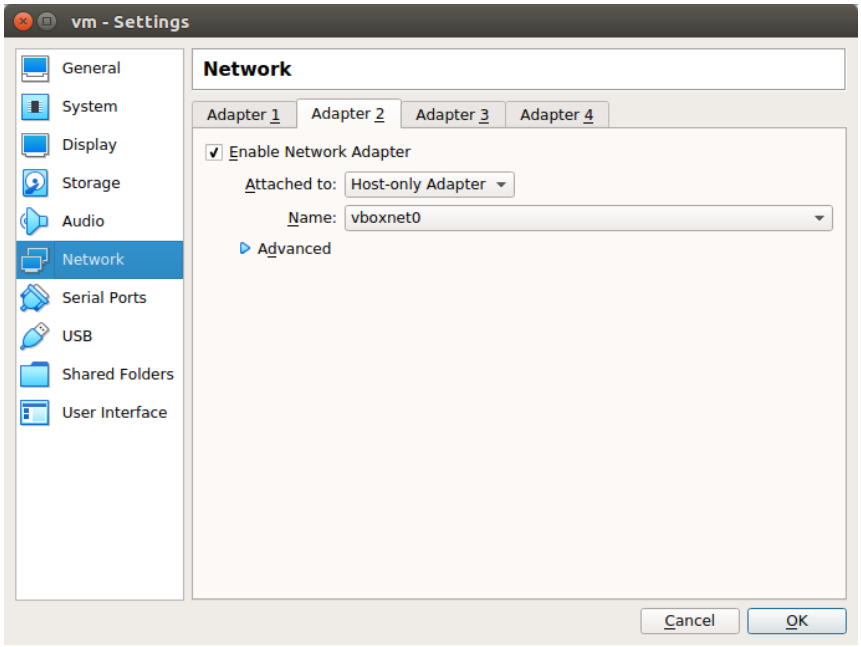


Şekil 3.8. Remnux ekran ayarları.

8- Network sekmesinde 4 farklı Ethernet kartı ayarı yapılabilir. Remnux'un güvenlik duvarı konumunda kullanılması sebebiyle bu sekmeden iki farklı Ethernet kartı ayarı yapılmaktadır. Şekil 3.9'da yer verilen ilk ethernet, NatNetwok adında ve NAT özelliği ile ağın internet tarafına bağlı olacak şekilde yapılandırılmaktadır. Şekil 3.10'da yer verilen ikinci ethernet ise vboxnet0 adında ve Host-only özellikli olarak istemci bilgisayar ile aynı ağda olacak şekilde yapılandırılarak aktif edilmektedir.

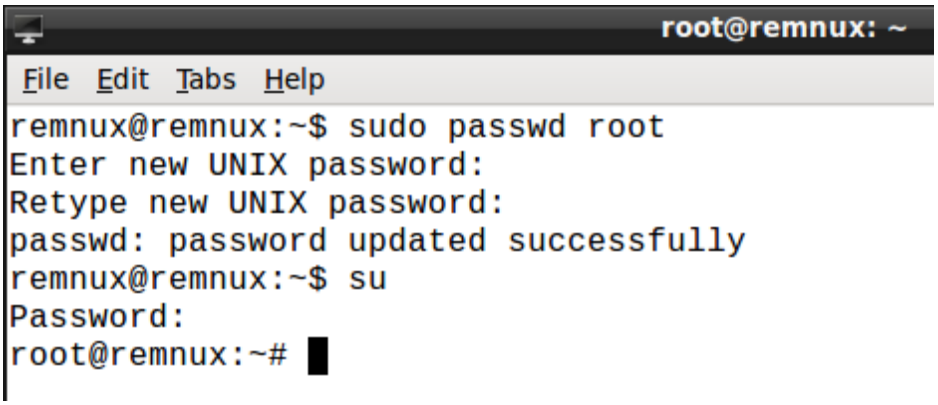


Şekil 3.9. Remnux nat özellikli ethernet gösterimi.



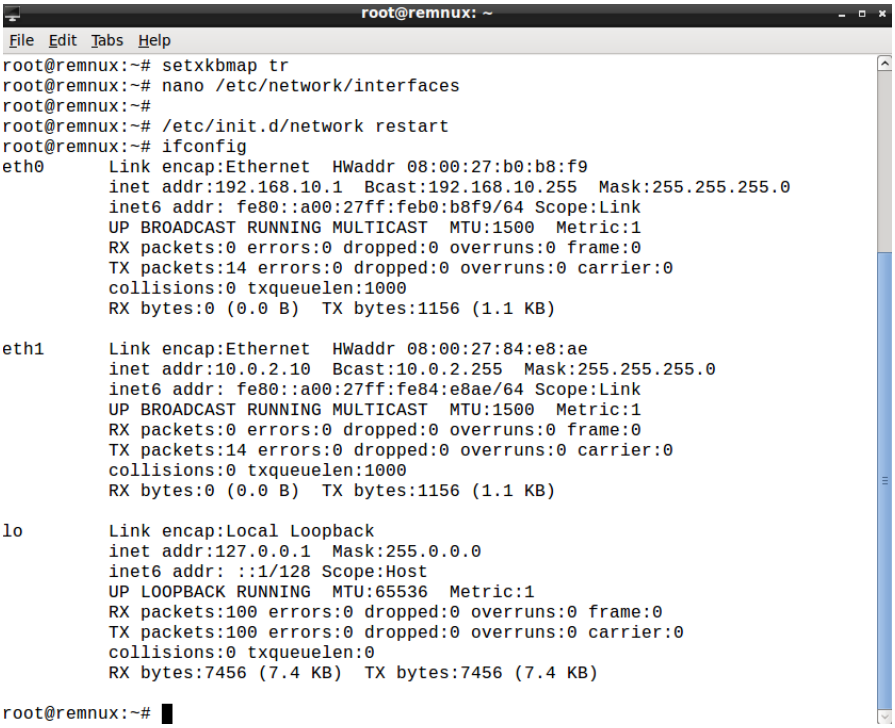
Şekil 3.10. Remnux host-only ethernet gösterimi.

9- Şekil 3.11'de yer verilen komutlar kullanılarak sisteme giriş yapılır, root parolası oluşturulur, root kullanıcısına geçiş yapılır.



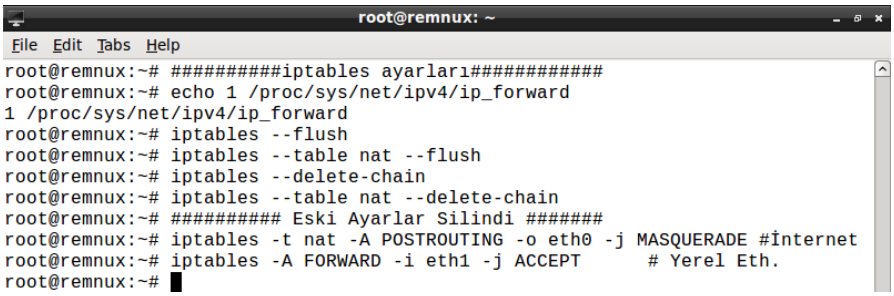
Şekil 3.11. Root kullanıcısına geçiş temel komutları.

10- "nano /etc/network/interface" komutu ile interface dosyası metin editörü ile açılır. İki ethernet kartı için ip adresi ve alt ağ maskesi girilir. Eth0 Host-only, eth1 NAT özellikli kartlardır. Remnux bilgisayarın ağ adres bilgileri Şekil 3.12'de verilmiştir.



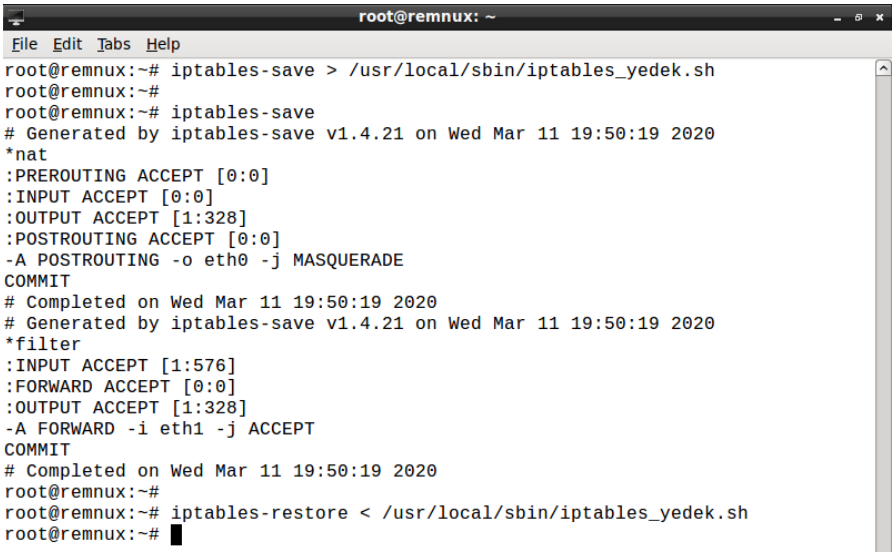
Şekil 3.12. Remnux ağ ayarları gösterimi.

11- Remnux üzerindeki Host-only özellikli Ethernet kartı zararlı yazılımın çalıştırılacağı istemci bilgisayar ile aynı ağdadır ve ağın varsayılan ağ geçididir. Bu ağdan gelen bağlantıların NAT özellikli Ethernet kartına yönlendirilmesi işlemi iptables ile gerçekleştirilir. Bu aşamada Şekil 3.13'te yer verilen komutlar kullanılarak yönlendir işlemini aktif etmek için ip_forward etkinleştirilir, yerel ağdan gelen bağlantıların (Host-only) kabul edilmesi ve maskelenerek internet ağına (NAT) gönderilmesi sağlanır.



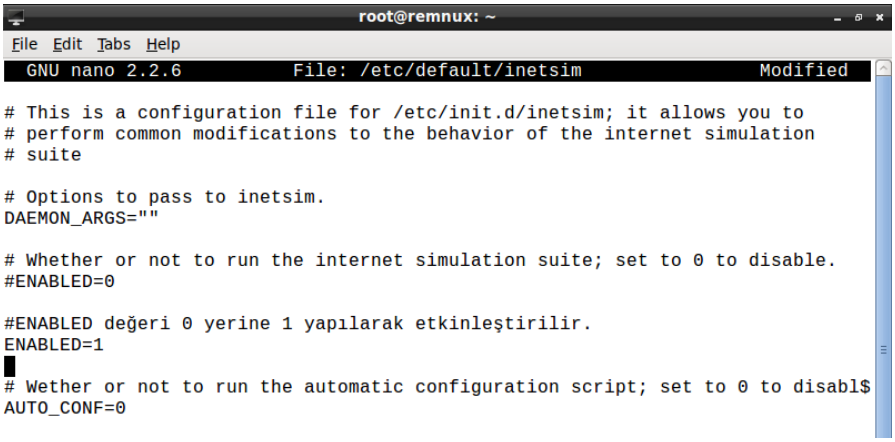
Şekil 3.13. Remnux iptables komutları gösterimi.

12- Iptables yapılandırması "iptables-save" komutu ile kayıt edilebilir veya "iptables-restore" komutu ile yenilenebilir. Şekil 3.14'de iptables ayarlarının kaydedilmesi, aktif ayarların görüntülenmesi, bir dosyadan ayarların tekrar aktif edilmesi için gerekli komutlara yer verilmektedir.



Şekil 3.14. Remnux iptables dosya içeriği ve kayıt edilmesi.

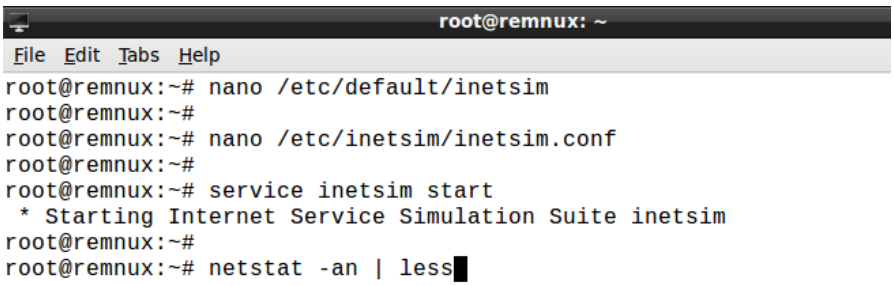
13- Inetsim, zararlı kodların dinamik olarak analiz edilmesi sırasında belirli ağ servisleri simüle edilerek zararlı kodun davranışı tespit edilebilen Linux temelli ücretsiz yazılım setidir. (http://halilozturkci.com/tag/malware-analizi/) Remnux içerisinde kurulu olarak gelir. "nano /etc/default/inetsim" komutu ile konfigürasyon dosyası açılarak Şekil 3.15'de yer verilen şekilde gösterildiği gibi "ENABLED" değeri 1 yapılarak aktif hale getirilmektedir.



Şekil 3.15. Remnux inetsim ayar dosyası.

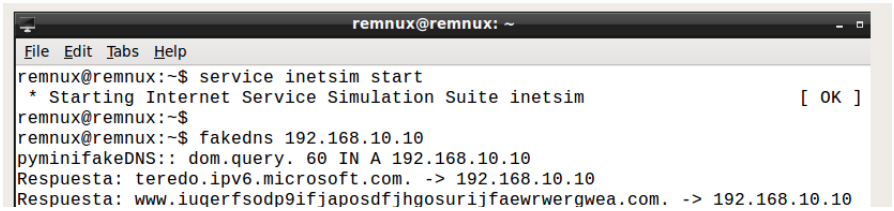
14- "nano /etc/inetsim/inetsim.conf" dosyası içerisinde simüle edilen ağ servisleri ve varsayılan ayarları bulunur. Konfigürasyon dosyası ile servislerin etkinleştirilmesi veya ayar değişikliği yapılmaktadır. Dinlediği servisler, servisler için kullandığı portlar bu dosyada yer alır. Bu dosyada başında "#" işareti olmayan servisler başlatılmaktadır. "service inetsim start/stop" ile servis başlatılması, "netstat -an | less" ile çalışan servislerin

listelenmesi komutları Şekil 3.16'da gösterilmektedir.



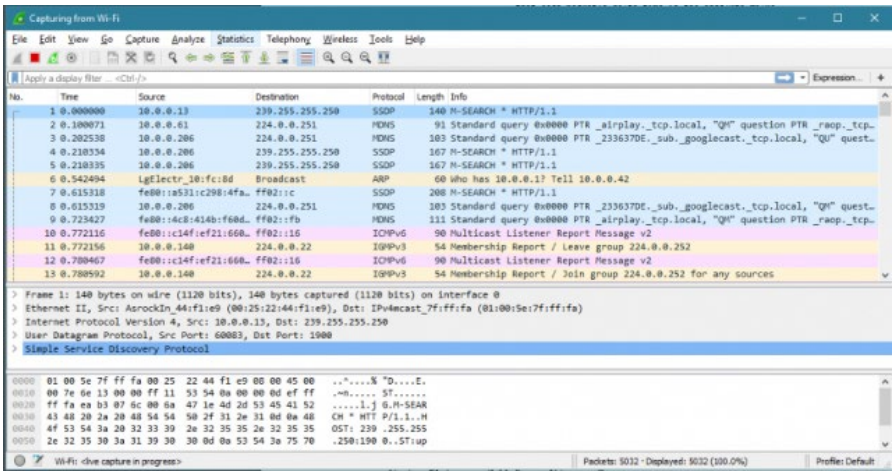
Şekil 3.16. Remnux inetsim servis çalıştırılması.

15- Fake dns, zararlı yazılımın dinamik analiz aşamasında bağlantı kurmaya çalıştığı DNS servis kayıtlarının tutulmasını sağlamaktadır. Şekil 3.17'de fakedns servisinin çalıştırılması ve DNS sorgu örneği gösterilmektedir.



Şekil 3.17. Remnux fakedns servis çalıştırılması.

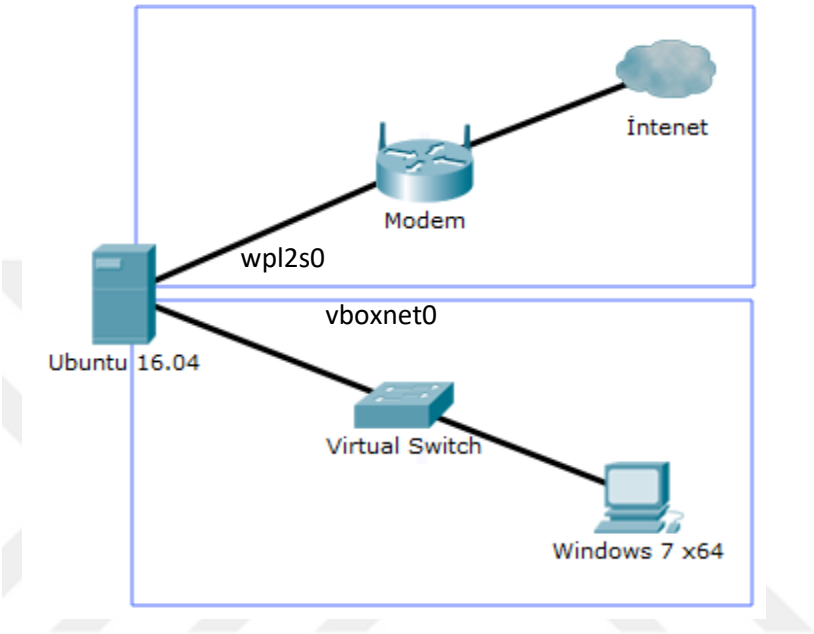
16-Wireshark, ağ trafiğinin anlık olarak izlenmesi, izlenen trafiğin kayıt edilmesi ve gerek duyulduğunda incelenmesini sağlamaktadır. Şekil 3.18'de örnek ekran görüntüsüne yer verilen wireshark bir hatayı çözmek amacı ile de kullanılabilmektedir. Bu işlem ile trafik izlenerek anlık filtreleme çözümleri kullanılarak sorun saptanmaya çalışılır (https://www.exploit-db.com/docs/40448).



Şekil 3.18. Wireshark görünümü.

3.2. CUCKOO SANDBOX ANALİZ ORTAMININ HAZIRLANMASI

Kurulum öncesi yapılan ayarlar, Şekil 3.19'da verilen topolojiye göre gerçekleştirilmektedir. Bu kapsamda kullanılan fiziksel bilgisayar üzerinde biri gerçek diğeri sanal olmak üzere iki ethernet yapılandırması Çizelge 3.2'de yer alan bilgilere göre gerçekleştirilmektedir.



Şekil 3.19. Cuckoo sandbox analiz ortamı ağ topolojisi.

Çizelge 3.2. Cuckoo sandbox analiz ortamı ip adres bilgileri.

Bilgisayar Türü	Fiziksel Bilgisayar		Sanal Bilgisayar 1
İşletim Sistemi	Ubuntu 16.04		Windows7 x64
Ethernet Adı	wlp2s0	Vboxnet0	
Ip Adresi	192.168.2.99	192.168.56.1	192.168.56.101
Alt Ağ Maskesi	255.255.255.0	255.255.255.0	255.255.255.0
Varsayılan Ağ Geçidi	192.168.2.1		192.168.56.1
DNS	195.175.39.39		195.175.39.39

Cuckoo kurulumu öncesi bazı yazılım paketlerinin kurulması gerekmektedir. Cuckoo temel bileşenleri tamamen Python'da yazılmıştır, bu nedenle uygun bir Python sürümünün yüklü olması gerekir. Cuckoo kurulum aşamaları sadece Python 2.7'yi tamamen desteklemektedir. Daha önceki Python sürümleri ve Python 3 sürümleri desteklenmemektedir.

Cuckoo'nun düzgün bir şekilde kurulmasını ve çalışmasını sağlamak için gerekli olan Python, MongoDB, PostgreSQL ve Virtualbox 6.1. kurulumu için Çizelge 3.3'de yer alan komutlar kullanılarak apt depolarından yazılım paketlerinin kurulumu gerçekleştirilir.

Cuckoo Sandbox çoğu sanallaştırma yazılımı çözümünü destekler. Analiz çalışmalarında kullanılmak üzere aşağıdaki işlem basamakları ile VirtualBox 6.1 kurulumu yapılır [40].

Çizelge 3.3. Cuckoo kurulumu hazırlık komutları

Python kullanımı için gerekli komut satırları	$ sudo apt-get install python python-pip python-dev libffi-dev
	$ sudo apt-get install python-virtualenv python-setuptools
	$ sudo apt-get install libjpeg-dev zlib1g-dev swig
MongoDB	$ sudo apt-get install mongodb
PostgreSQL	$ sudo apt-get install postgresql libpq-dev
Virtualbox 6.1. için depo anahtarının eklenmesi	sudo sh -c 'echo "deb [arch=amd64]
	https://download.virtualbox.org/virtualbox/debian $(lsb_release -sc) contrib" >>
Virtualbox depo anahtarının eklenmesi	wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc -O- | sudo apt-key add -
Sistem önbelleğinin	sudo apt-get update
Virtualbox 6.1.	sudo apt-get install virtualbox-6.1

Tcpdump Kurulumu: Analiz aşamasında kötü amaçlı yazılım tarafından gerçekleştirilen ağ etkinliğini izlemek, trafiği yakalamak, filtrelemek ve bir dosyaya kayıt etmek için düzgün yapılandırılmış bir ağ dinleyicisine ihtiyacınız bulunmaktadır. Bu işlemler tcpdump ile gerçekleştirilmektedir. Tcpdump root yetkileri ile çalıştırılır, ancak

Cuckoo'nun root yetkileri ile çalışması istenilmemektedir. Bu nedenle tcpdump için Çizelge 3.4'de yer alan komut satırları ile kurulum ve ayrıcalık ayarları yapılır.

Çizelge 3.4. Tcpdump kurulum komutları

sudo apt-get install tcpdump
sudo groupadd pcap
sudo usermod -a -G pcap cuckoo
sudo chgrp pcap /usr/sbin/tcpdump
sudo setcap cap_net_raw,cap_net_admin=eip
$ getcap /usr/sbin/tcpdump

Volatility Kurulumu: Volatilite, bellek dökümlerinde adli analiz yapmak için kullanılan bir araçtır. Zararlı yazılımın çalıştırıldığı işletim sisteminde bellek üzerindeki değişikliklerinin izlenmesini ve rootkit teknolojisinin varlığını tespit edebilmektedir.

Düzgün çalışması için Cuckoo, Volatility'nin en az 2.3 sürümünü gerektirir, ancak en son sürümü olan Volatility 2.6 önerilir.

- sudo apt-get install volatility

M2crypto ve SWIG Kurulumu :SWIG, C ve C ++ ile yazılmış programları çeşitli üst düzey programlama dillerine bağlayan bir yazılım geliştirme aracıdır.

- sudo apt-get install swig
- sudo pip install m2crypto==0.24.0

Guacd kurulumu: Cuckoo web arayüzünün uzaktan kullanılabilmesi amacıyla RDP, VNC ve SSH için çeviri katmanı sağlayan isteğe bağlı bir hizmettir.

- sudo apt install libguac-client-rdp0 libguac-client-vnc0 libguac-client-ssh0 guacd

Kullanıcı Oluşturulması :Kurulum aşamasında "cuckoo" adında bir kullanıcı oluşturulmadıysa aşağıdaki komutlar ile oluşturulur ve VirtualBox kullanmak için vboxusers grubuna dahil edilir.

- sudo useradd cuckoo

- sudo usermod -a -G vboxusers cuckoo

Cuckoo Kurulumu: Öncelikle pip ve setuptools kurulumu sonrasında cuckoo kurulumu yapılmaktadır.

- pip install -U pip setuptools
- pip install -U cuckoo

Cuckoo Yapılandırma İşlemleri

"cuckoo -d" komutu ile Cuckoo varsayılan ayarları ile ilk çalıştırma işlemi yapılır. Bu aşamada cuckoo yapılandırma dosyalarının isteğe göre yapılandırılması gerekmektedir.

Cuckoo temel yapılandırma dosyaları aşağıdaki gibidir:

cuckoo.conf : Genel davranış ve analiz seçenekleri yapılandırma dosyasıdır.

auxiliary.conf : Yardımcı modülleri etkinleştirme ve yapılandırma dosyasıdır.

<machinery> .conf : Sanallaştırma yazılımı seçeneklerini tanımlamak için kullanılan dosyadır(dosya cuckoo.conf dosyasında seçilen makine modülü ile aynı ada sahiptir).

memory.conf : Bellek yapılandırma dosyasıdır.

processing.conf : Process modüllerini etkinleştirme ve yapılandırma dosyasıdır.

reporting.conf : Rapor biçimlerini etkinleştirme veya devre dışı bırakma işlemleri yapılandırma dosyasıdır.

Cuckoo'nun çalışması için en azından cuckoo.conf ve <machinery>.conf dosyalarının düzenlenmesi gerekmektedir.

cuckoo.conf Dosyası

Dosya içerisinde bulunan özellikler genel olarak açıklayıcı yorum satırları içermektedir. Bunun yanında aşağıdaki özellikler mutlaka ayarlanması gereken özelliklerdir.

machinery: Cuckoo tarafından kullanılacak sanallaştırma yazılım modülünün adı belirtilir. Uzantısız modül adı yazılır.

machinery = virtualbox

machinery = vmware

[resultserver]

ip = 192.168.56.1

Analiz edilen makinelerin sonuç bilgilerinin döndürüleceği ana makinenin ip adresidir.

[databese]

connection =

Cuckoo'nun dahili veritabanına nasıl bağlanılacağı tanımlanır.

auxiliary.conf

Zararlı yazılım analizi ile aynı anda çalışan script dosyalarını ve seçeneklerini tanımlar.

virtualbox.conf

Cuckoo'nun analiz aşamasında etkileşime gireceği sanallaştırma yazılımını tanımlar.

Her sanallaştırma yazılımının ayrıntılarıyla tanımlandığı özel bir yapılandırma dosyası vardır. Bu yapılandır dosyaları vmware.conf veya virtualbox.conf şeklinde tanımlanır.

Kullanılacak sanallaştırma yazılımı yolu, ağ ara yüzü adı, sanal makine adı, sanal makine platformu, ip adresi, snapshot adı, bu dosyada belirtilir.

path = /usr/bin/VBoxManage

interface = vboxnet0

machines = cuckoo1

platform = windows

ip = 192.168.56.101

snapshot = Snapshot1

memory.conf

Bellek analizi amacıyla volatility yazılımı kullanılacak ise processing.conf dosyasında [memory] sekmesinden etkinleştirilmelidir. Analiz amacıyle memory_dump kullanılacak ise cuckoo.conf dosyasından memory_dump etkinleştirilmelidir.

processing.conf

[memory]

enabled = yes

memory.conf

[basic]

Guest_profile = Win7SP1x86, WinXPSP3x86 vb.

processing.conf

Analiz aşamasında toplanan verilerin hangi modüllere göre işleneceğinin belirlendiği dosyadır. Bu dosya içerisinde işleme modülleri etkinleştirilir veya devre dışı bırakılır.

Örneğin;
[virustotal]

enabled = yes

Şüpheli yazılımın virustotal tarafından incelenmesi işleminin aktif ya da pasif yapılmasını sağlamaktadır.

reporting.conf

Rapor işlemleri hakkında gerekli tanımlamaların, etkinleştirme veya devre dışı bırakma işlemlerinin yapıldığı dosyadır.

Örneğin;

[mongodb]

enabled = no

Mongodb veritabanının rapor aşamasında aktif ya da pasif yapılmasını sağlamaktadır.

Yara Kurulumu: Yara, zararlı kodlar üzerinde çalışan uzmanların, bu zararlı kodları tanımlamalarına ve sınıflandırmalarına imkan tanımak için geliştirilmiş bir araçtır [41]. Çizelge 3.5'de yara kurulumu için gerekli komut satırları verilmektedir.

Çizelge 3.5. Yara kurulum komutları

sudo apt-get install autoconf libtool libjansson-dev libmagic-dev libssl-dev -y
wget https://github.com/plusvic/yara/archive/v3.4.0.tar.gz -O yara-3.4.0.tar.gz
tar -zxf yara-3.4.0.tar.gz$ cd yara-3.4.0$ ./bootstrap.sh
./configure --with-crypto --enable-cuckoo --enable-magic
make
sudo make install
yara -v

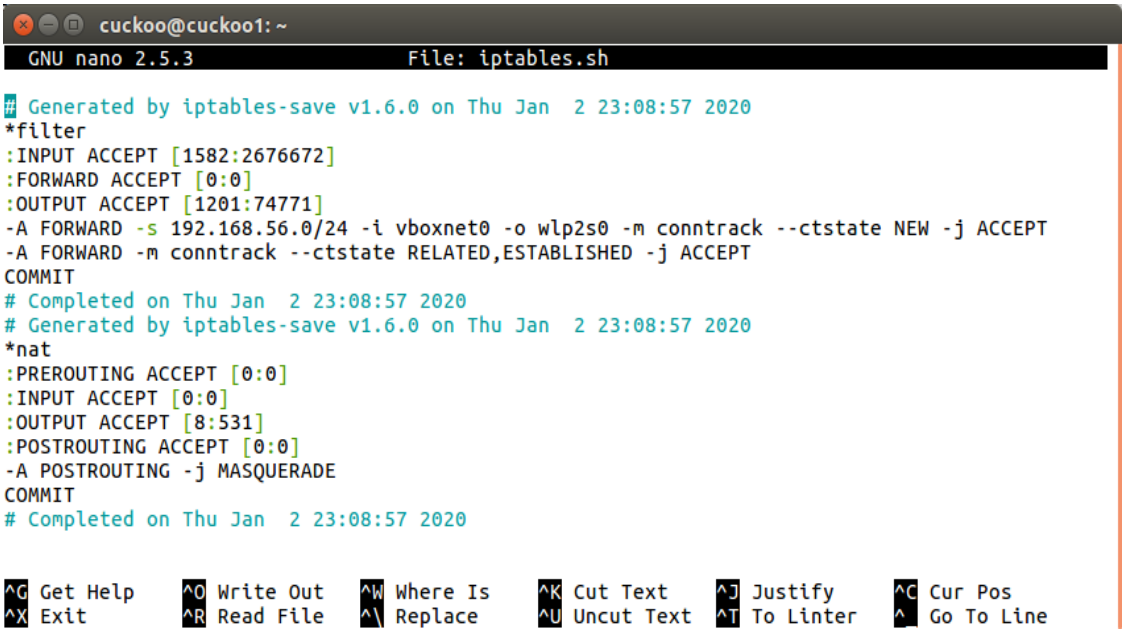
Iptables Ayarları: Host-only olarak yapılandırılan bir ağın internet bağlantısı bulunmamaktadır. Bu ağın internete bağlanabilmesi için bağlı olduğu ana makinenin ethernet ara yüzleri arasında yönlendirme yapılması gerekmektedir. Bu yönlendirme için öncelikle ip_forward özelliği etkinleştirilir ve iptables ayarları yapılmaktadır.

iptables-save komutu ile aktif iptables ayarları görüntülenir.

iptables-save > iptables.sh komutu ile aktif ayarlar iptables.sh adında bir dosyaya kayıt edilir.

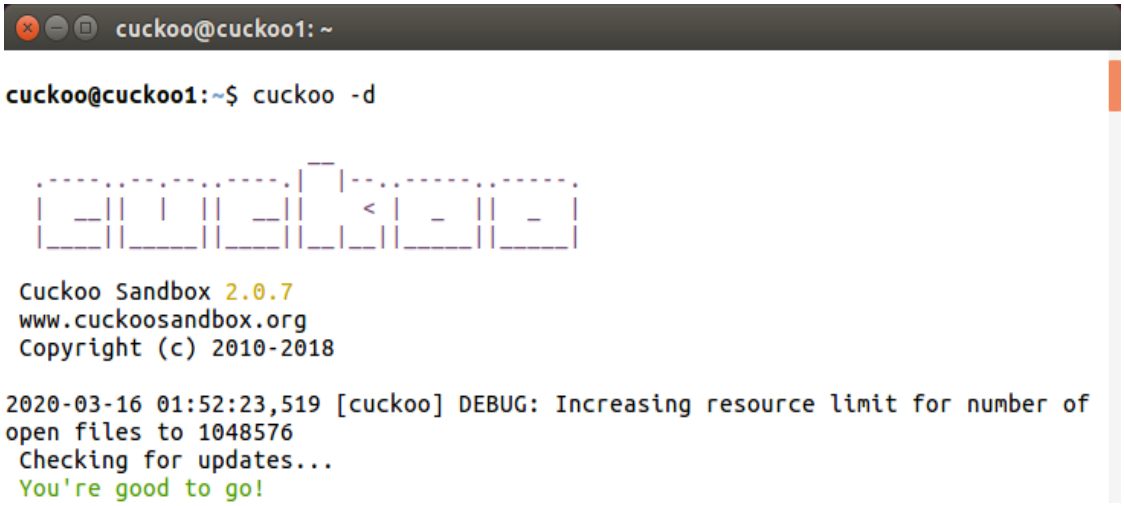
iptables-restore < iptables.sh komutu ile iptables.sh adında bir dosyadan iptables ayarları aktifleştirilir.

nano iptables.sh komutu ile Şekil 3.20'de yer verildiği gibi dosya içeriği görüntülenebilmektedir.



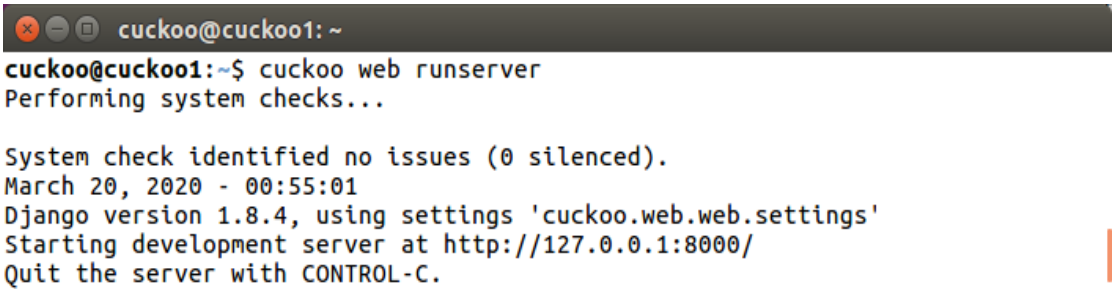
Şekil 3.20. Ubuntu 16.04 iptables konfigürasyon dosyası.

Cuckoo Sandbox Çalıştırılması: Linux terminal üzerinden Şekil 3.21'de gösterildiği gibi cuckoo -d komutu ile servis çalıştırılır.



Şekil 3.21. Cuckoo servisinin çalıştırılması.

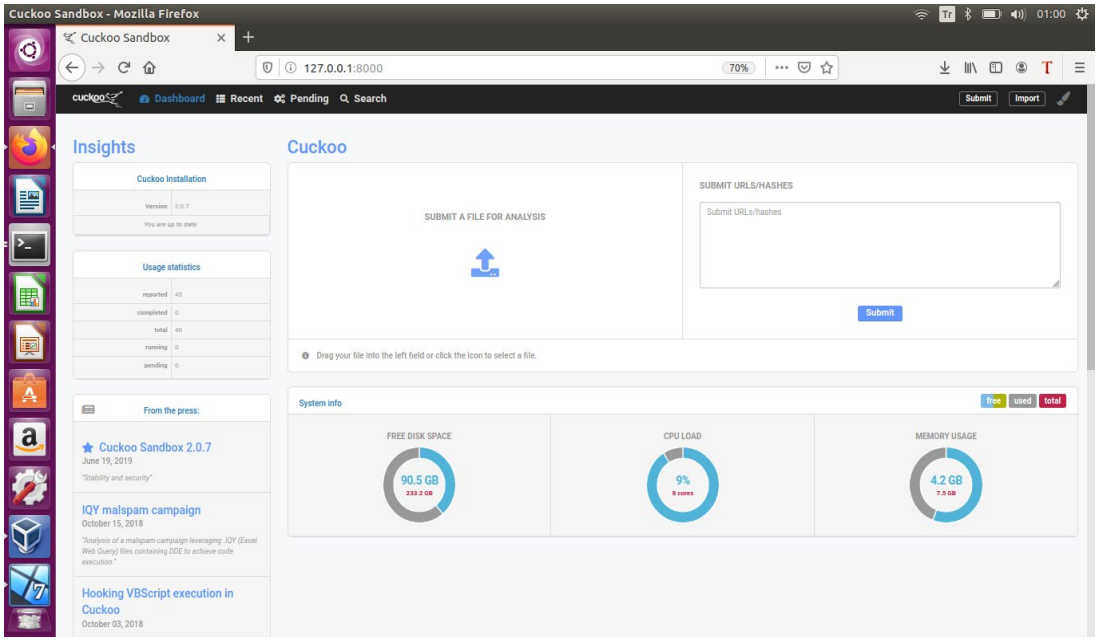
Çalışan yazılıma web servisi üzerinden analiz edilecek yazılımın aktarılabilmesi için Şekil 3.22'de yer verildiği gibi cuckoo web runserver komutu kullanılır.



Şekil 3.22. Cuckoo web serverın çalıştırılması.

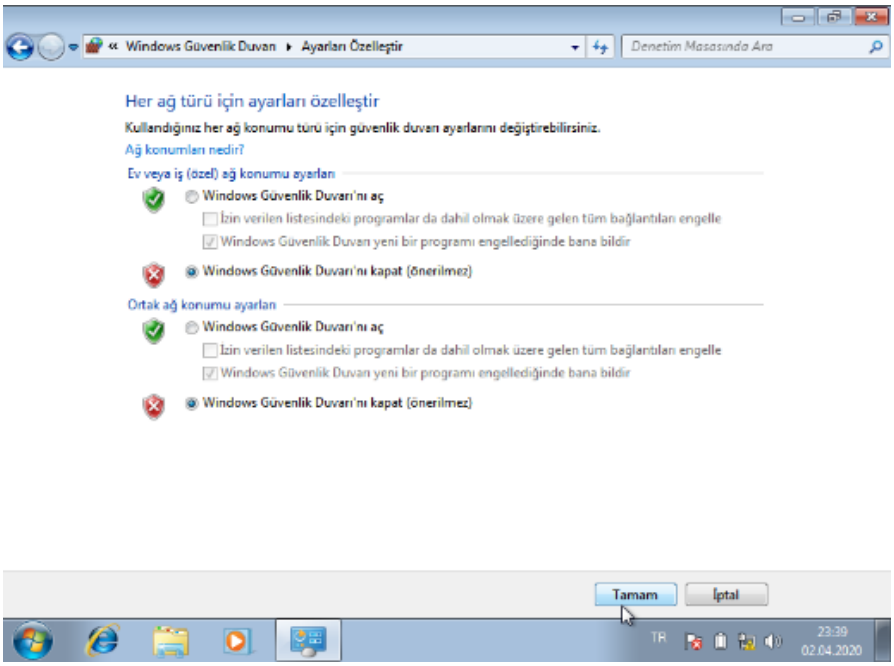
Sanal makine üzerinde yazılım analizi yapmak üzere ana makinede herhangi bir internet tarayıcısında localhost üzerinde 8000 portundan cuckoo açılır.

cuckoo web runserver ipadresi:8000 şeklinde yazılan bir komut ile cuckoo servisine network üzerinden bağlantı kurularak analiz yapılabilir. Şekil 3.23'te sandbox giriş penceresi gösterilmiştir.



Şekil 3.23. Cuckoo sandbox giriş penceresi.

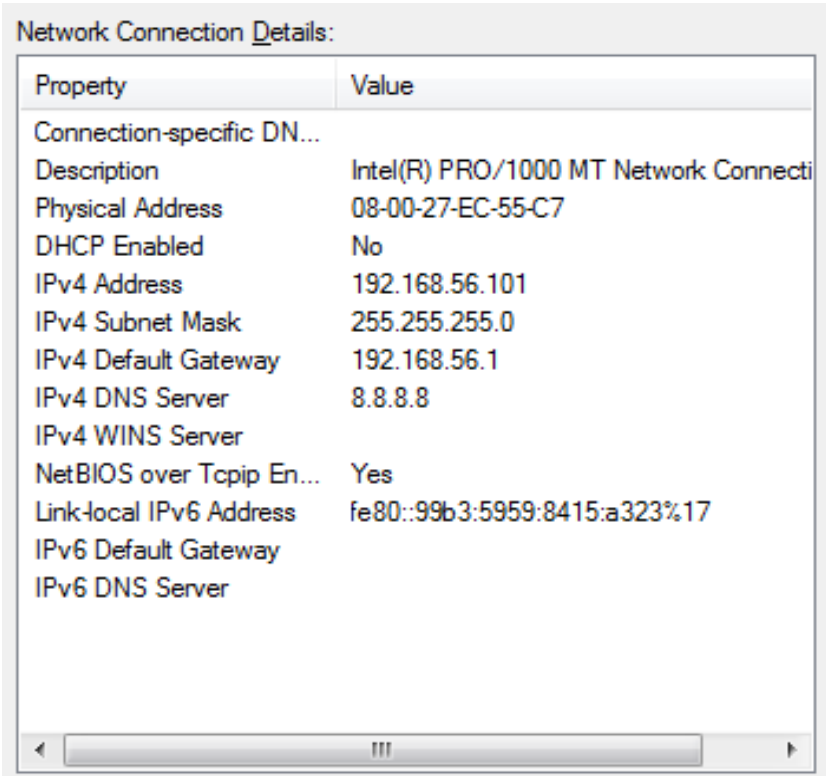
İstemci makine ayarları: Şekil 3.24'de yer verildiği gibi ana makine ve çalışan cuckoo servisi tarafından yapılan bağlantıları engellememek amacıyla güvenlik duvarı devre dışı bırakılmaktadır.



Şekil 3.24. İstemci güvenlik duvarı ayarları.

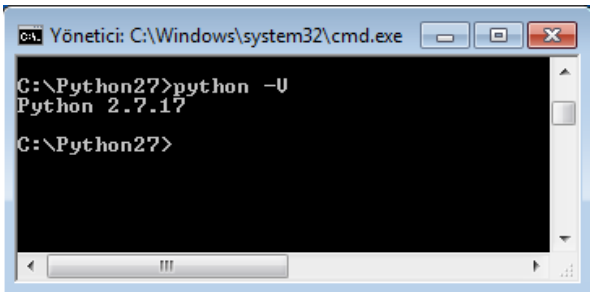
Test ortamı ana bilgisayarının bağlı olduğu network üzerinden herhangi bir sorun olmaması için ana bilgisayar ile istemci bilgisayarlar arasında Host-Only bağlantı kurulmaktadır. Host-only özellikli vboxnet0 sanal network arayüzü üzerinden ana

makineye bağlanmak üzere Şekil 3.25'de gösterilen ağ ayarları yapılandırılır.



Şekil 3.25. İstemci ağ ayarları.

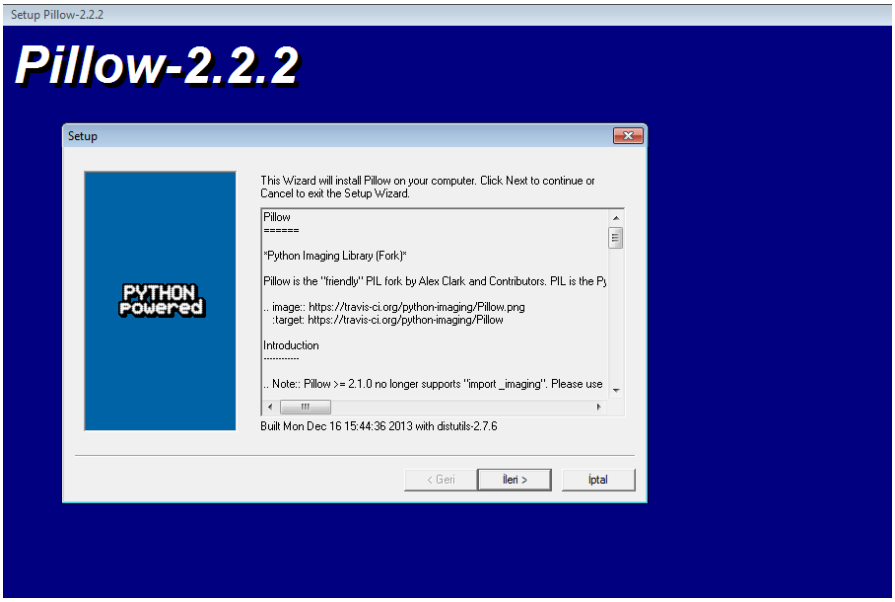
Analiz amacıyla kullanılan cuckoo servisimiz python tabanlı bir yazılımdır. Bu nedenle ana bilgisayar ile istemci bilgisayarın iletişimi amacıyla istemci bilgisayara python resmi sitesinden Şekil 3.26'da sürüm bilgisi gösterilen Python2.7 kurulumu yapılır.



Şekil 3.26. İstemci Python sürüm bilgisi.

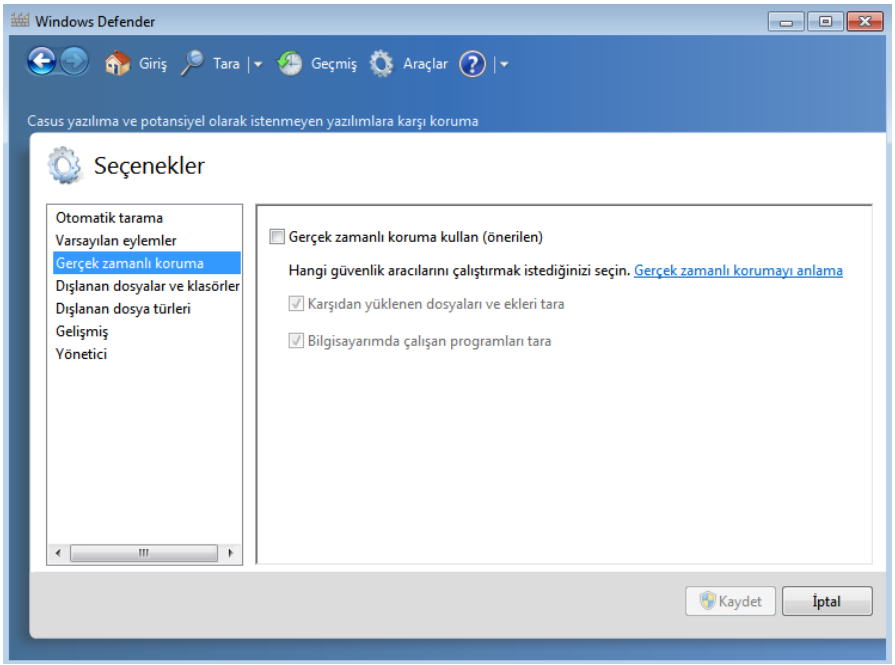
Ana bilgisayar ile istemci arasındaki python tabanlı iletişim Pillow kütüphanesi kurulumu yapılır. Pillow (Python Imaging Library - PIL), Python programlama dili için geliştirilen, açık kaynak kodlu grafik işleme kütüphanesidir. Bu kütüphane, içinde barındırdığı hazır fonksiyonlar sayesinde programcıya üstün bir grafik işleme imkânı sunmaktadır. Birçok grafik türünü açıp kaydetme yeteneği ile birlikte çizim, düzenleme, filtreleme gibi işlemlerde kullanılabilecek fonksiyonlara sahiptir [42]. İstemci makineye

kurulan Python 2.7 ile uyumlu Şekil 3.27'de gösterilen Pillow kütüphanesi kurulumu yapılır.



Şekil 3.27. İstemci Python-Pillow kurulumu.

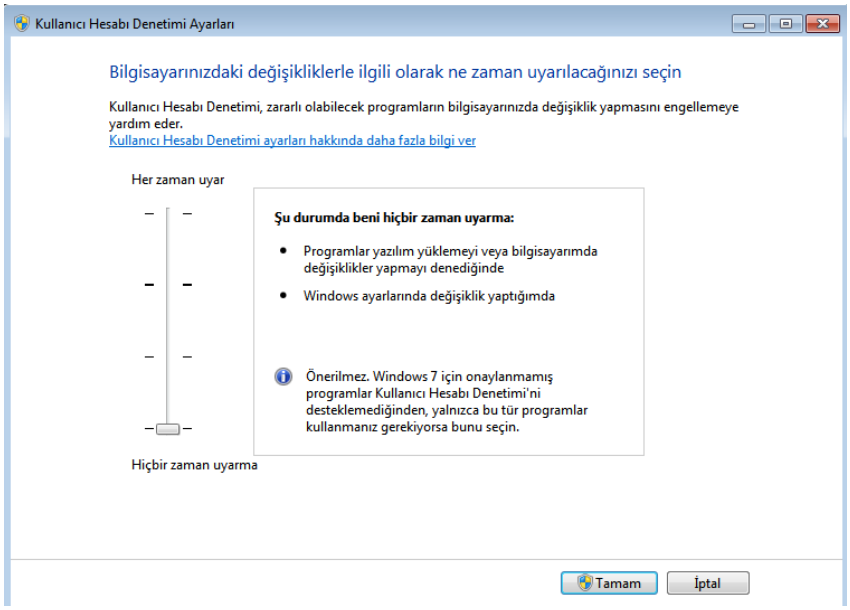
Amacımız analiz edilen yazılımın işletim sistemi üzerinde oluşturduğu etkiyi görmek olduğu için Şekil 3.28'de gösterilen Windows Defender ya da varsa kurulu diğer anti virüs yazılımları devre dışı bırakılır.



Şekil 3.28. İstemci antivirüs ayarları.

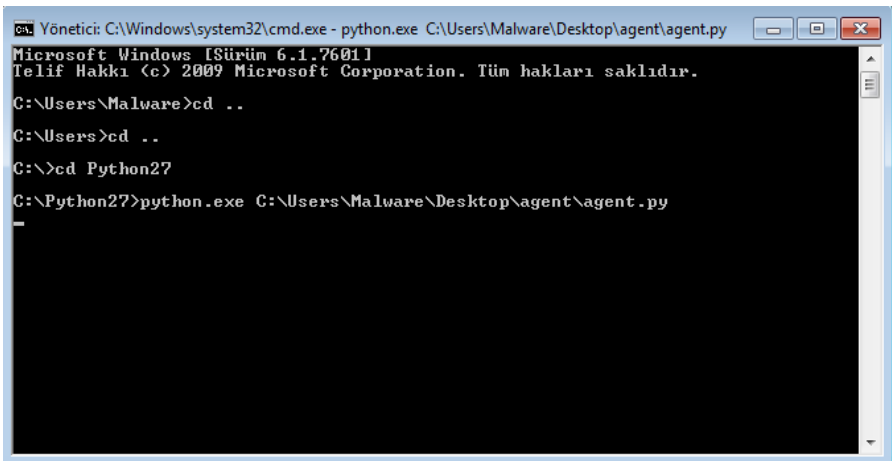
Kullanıcı hesabı denetimi (User Account Control – UAC), zararlı olabilecek programların

bilgisayar üzerinde değişiklik yapmasına engel olmaktadır. Bu nedenle kullanıcı hesabı denetimi, Şekil 3.29'da gösterildiği gibi en alt seviye olan hiçbir zaman uyarma seviyesine getirilir.



Şekil 3.29. İstemci kullanıcı hesap denetim ayarları.

Analiz süreci başlatıldığında kapalı durumdaki sanal istemci Virtualbox üzerinden çalıştırılır. Ana makinenin analiz sürecini yürütebilmesi amacıyla istemci makine üzerinde python betiği çalıştırılması gerekmektedir. Bu betik ana makinede cuckoo dizini altında agent dizininde bulunur. Cuckoo ayar dosyası içerisinde bulunan agent.py dosyası istemci makineye kopyalanarak Şekil 3.30'da gösterildiği gibi çalıştırılır.



Şekil 3.30. İstemci agent.py çalıştırılması.

Yukarıdaki ayarlar aktif halde iken Snapshot1 adında snapshot alınır. Analiz işlemi başlatıldığında istenilen tüm ayarları üzerinde barındıran Snapshot1 çalıştırılmaktadır.

4. ZARARLI YAZILIM ANALİZLERİ

4.1. REMNUX İLE NETWORK TABANLI ZARARLI YAZILIM ANALİZİ

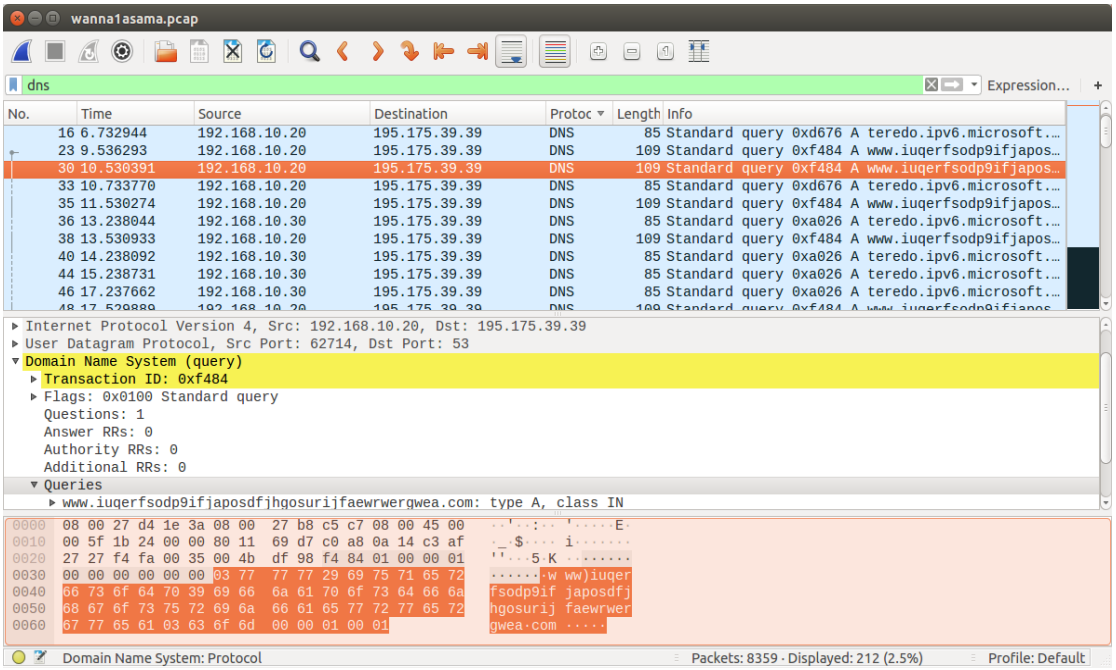
Ağ trafiğinin görüntülenmesi, ağ aygıtlarına herhangi bir araç veya istemci yazılımı yüklenilmesine gerek kalmadan ağ üzerindeki hareketleri izlemenin ideal bir yoludur [43]. Bilgisayar ağlarında güvenli olmayan eski sistemlerin bağlı olduğu veya güvensiz olduğu kabul edilen SMB1 gibi servislerin sürekli kontrol edilmesi için de çok yararlı bir seçenektir.

Bilgisayar ağları üzerindeki iletişimi izlemenin en kolay yollarından biri, port aynalama (port mirror) bağlantısı kurmaktır. Port aynalama işlemi, bir porttan geçen trafiğin kopyasının bir başta porta kopyalanmasıdır. Böylece port üzerinden geçen trafik izlenebilir. Bu yöntem, tüm ağ trafiği akışlarına ve paket yüklerine erişilmesini sağlamaktadır.

Yapılan analiz çalışmasında, Remnux bilgisayar istemci ile internet arasında köprü görevi görmektedir. Bu sebeple istemci üzerinde oluşan tüm ağ trafiği Remnux üzerinden geçeceği için yine istemcinin tüm ağ trafik akışı izlenebilir hale gelmektedir. Zararlı yazılımın analiz edileceği istemcinin analiz aşamasında şifrelenmesi sebebiyle gerekli sonuçlar istemci üzerinden alınamamaktadır.

Ağ trafik akışından anlamlı bilgiler elde etmek için ağ paketlerini işleyebilen bir uygulamaya ihtiyaç duyulmaktadır. Wireshark, ağ trafiğinin bir grafik arayüz üzerinden izlenmesini sağlayan, pek çok zaman hayat kurtarıcı öneme sahip bir programdır. Uygulamanın kurulu olduğu bilgisayar üzerinden anlık network trafiği izlenebileceği gibi, daha önce kaydedilmiş dosyaların incelenmesi amacı ile de Wireshark kullanılabilmektedir [44]. Wireshark, açık kaynaklı paket analiz yazılımıdır, bilgisayara bağlı olan ethernet kartlarındaki tüm verilerin analiz edilmesini ve daha önceden kaydedilmiş olan network trafiklerinin de incelemesini sağlamaktadır. Şebeke problemlerinde sorun çözmek, güvenlik problemlerini sınamak, uygulamaya konan protokollerde oluşan hataları onarmak veya arındırmak, ağ protokolünün içerisindeki bilgileri öğrenebilmek için wireshark programı kullanılmaktadır [45].

Yapılan çalışmada wannacry yazılımının ağ hareketleri incelenmektedir. Yazılım çalıştırıldığında Şekil 4.1'de yer verildiği gibi öncelikle www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com adresi için DNS sorgusu yapılmaktadır.



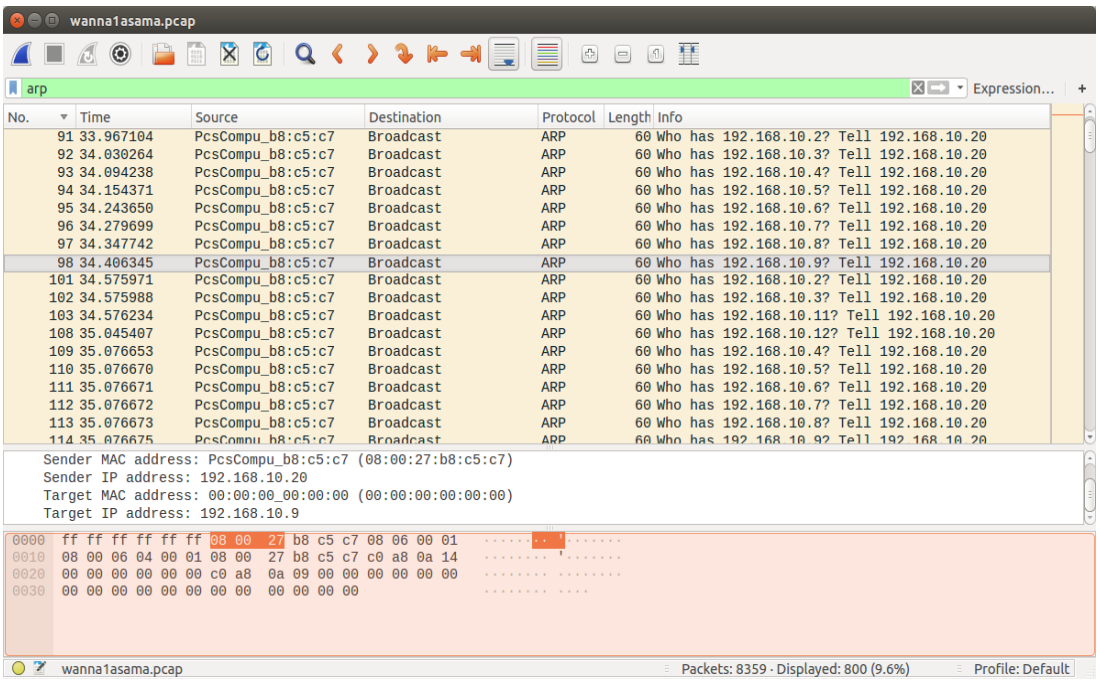
Şekil 4.1. Wireshark DNS bilgileri.

Bu aşamada zararlı yazılımın çalıştırıldığı makine içerisindeki dosyalar şifrelenmeye başlamaktadır. Şifreleme işleminin tamamlanması ile birlikte ekrana Şekil 4.2'de gösterilen uyarı mesajı gelmektedir. Bu mesaj ile bağlantı bilgileri, ödenmesi gereken fidye miktarı, ödeme için tanınan süre ve dosyaların tamamen kaybetmeden önce kalan süre gibi açıklama bilgileri görüntülenmektedir.



Şekil 4.2. WannaCry kilitleme ve bilgilendirme penceresi.

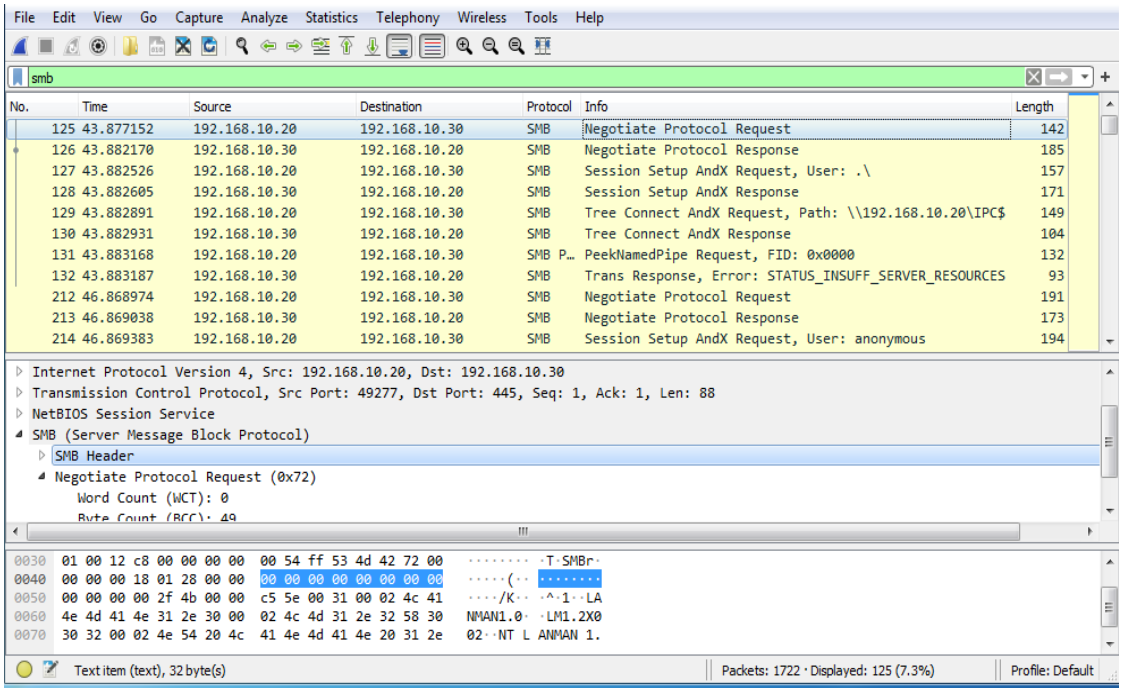
Zararlı yazılımın çalıştırılması ile birlikte istemci bilgisayar ağ üzerinde bulunan diğer bilgisayarlara aynı zararlı yazılımı bulaştırabilmek, işletim sistemlerinde açık olup olmadığını kontrol etmek amacıyla aynı ağa bağlı olabilecek tüm ip adreslerine Şekil 4.3'de görüldüğü gibi ARP sorgusu yapmaktadır. ARP sorgusu ile ağ içerisinde ip adresleri bilinen makinelerin ethernet kartlarının 48 bitlik fiziksel adresi alınarak aktif durumdaki makineler öğrenilmiş olunur.



Şekil 4.3. WannaCry ARP sorguları.

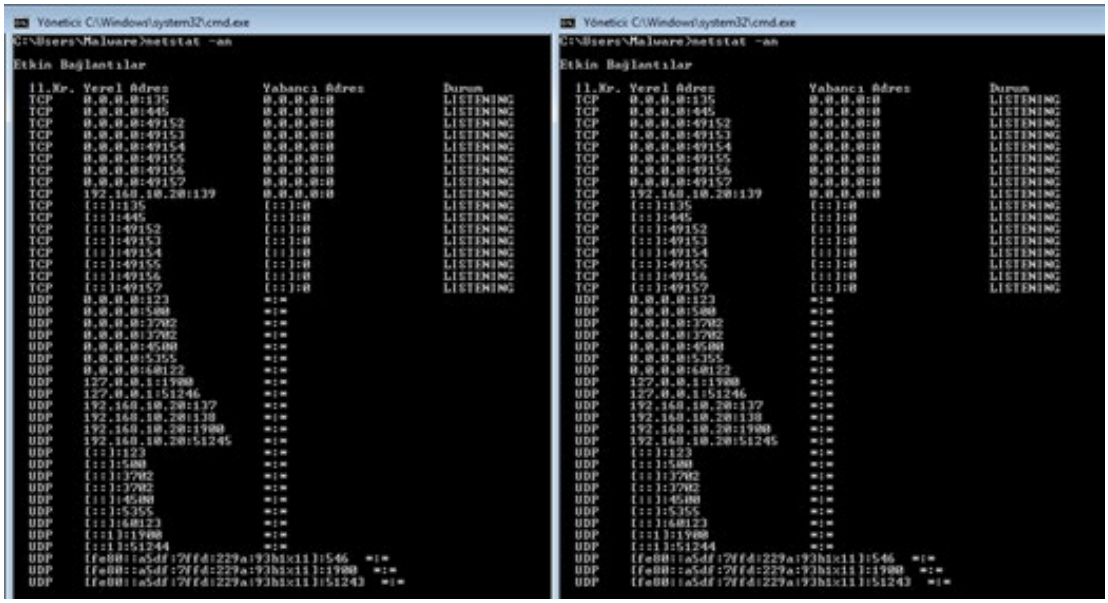
Ağ içerisinde aktif olduğu belirlenen makineler ile SMB 445 portu üzerinden bağlantı kurulmaktadır. Aynı güvenlik açıklarından faydalanarak ağ içerisindeki diğer makinelere de ulaşılmaktadır. Zararlı yazılımın çalıştırıldığı 192.168.10.20 ip adresli makinenin ağ içerisinde aktif olarak bulunan 192.168.10.30 ip adresli makine ile SMB protokolü ile bağlantı kurduğu görülmektedir.

Ağda bulunan iki farklı makinenin görevleri ters çevrilerek zararlı yazılım 192.168.10.30 ip adresli makinede çalıştırılmıştır. Aşağıdaki ekran görüntüsü ile ağda normal işlemlerine devam eden 192.168.10.20 ip adresli makinenin zararlı yazılımın çalıştırılan bir makine tarafından nasıl etkilendiği Şekil 4.4'de görülmektedir. Bu işlem için netstat -an komutu kullanılmaktadır. Netstat komutu, ağ bağlantılarını, yönlendirme tablosunu, arabirim istatistiklerini ve benzer ağ bağlantısı bilgileri ile ilgili ayrıntılı bilgiler verebilen bir konsol komutudur. -a parametresi ile tüm TCP ve UDP bağlantılarını ekrana basar. --n parametresi ile tüm bağlantılar rakamsal olarak görüntülenmektedir.



Şekil 4.4. WannaCry ağdaki diğer bilgisayarlara SMB ile bağlantı kurulması.

Başlangıç aşamasında 445 numaralı portun dinleme modunda olduğu ve herhangi bir makine ile bağlantı kurulmadığı görülmektedir. Zararlı yazılım 192.168.10.30 da çalıştırılmış ve ARP sorgusu ile ağdaki 192.168.10.20 ip adresli makinenin aktif olduğu görülmüştür. Bu makinede bulunan açık ile 445 portuna 34 farklı bağlantının aktif olarak yapıldığı Şekil 4.5'de görülmektedir.



Şekil 4.5. WannaCry bulaşma öncesi ve sonrası çalışan ağ servisleri.

Yapılan analiz işleminde bir makinede herhangi bir yazılımın çalıştırılması ile başlatılan ağ hareketleri analiz edilmektedir. Analiz ile çalıştırılan kullanıcıdan bağımsız ağ hareketleri gözlenmektedir. Bu kapsamda yapılan DNS sorguları, ARP sorguları, SMB protokol bağlantıları izlenerek yazılımın istek dışı ağ işlemlerinden dolayı zararlı yazılım olduğu sonucuna varılmaktadır.

Yukarıda yapılan analiz işlemi Petya zararlı yazılımı çalıştırılarak tekrarlanmıştır. Bu kapsamda Petya zararlı yazılımının çalıştırılması sonucu herhangi bir ağ hareketi kayıt edilememektedir. Petya'nın çalıştırılması ile kurulan Remnux analiz çalışmasının zararlı yazılımın ağ hareketleri olması durumunda etkili olduğu, ağ hareketlerinin olmadığı durumlarda ise etkili olmadığı görülmektedir.

4.2. CUCKOO SANDBOX İLE WANNACRY ZARARLI YAZILIM ANALİZİ

Analiz işlemi, Ubuntu dağıtımına yüklenen Cuckoo Sandbox 2.0.7 servisinin Virtualbox 6.1 üzerinde Windows7 sanal işletim sistemini çalıştırması ile gerçekleştirilmektedir.

malshare.com web sitesinde ve any.run online sandbox web sitesinde yapılan tarama ile alınan 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c isimli Wannacry zararlı yazılımı 127.0.0.1:8000 numaralı localhost portunda çalıştırılan kum havuzu ile analiz edilmiştir.

WannaCry'nin kendine has özellikleri bulunmaktadır. İşletim sistemini tamamen ele

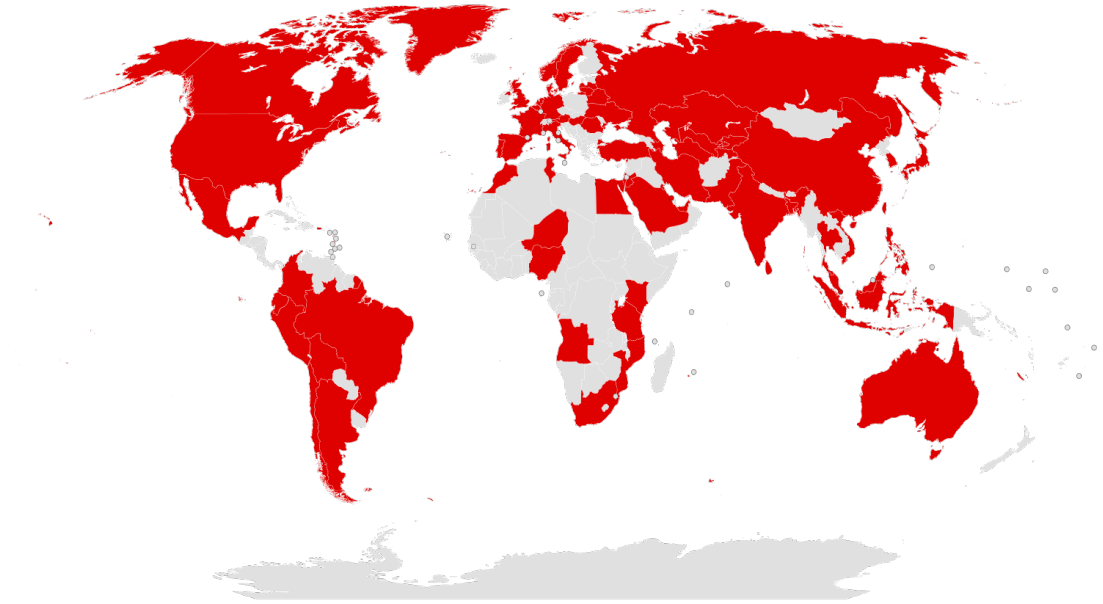
geçirmek için dosyalardan birine, bilgisayara veya ağa ulaşması yeterlidir. Virüs ağa veya bilgisayar ekipmanına girmeyi başardığında, belirli koşullar altında Windows işletim sistemine sahip diğer bilgisayarlara yayılır. Süreç otomatiktir ve insan müdahalesi gerekli değildir. Kötü amaçlı yazılımın giriş yolu, bir e-postadaki yürütülebilir bir dosya olabilir [46]. WannaCry, enfeksiyon aşamasında EternalBlue kullanmaktadır. EternalBlue, 14 Mart 2017 tarihinde Microsoft tarafından yayınlanan ve MS17-010 güvenlik bülteninde açıklanan SMB güvenlik açığından yararlanmaktadır. Bu güvenlik açığı, saldırganların bir SMBv1 sunucusuna özel hazırlanmış iletiler göndererek ve kodlanmamış Windows sistemlerinin TCP ve 139 bağlantı noktalarına bağlanan uzak kod yürütmesine olanak tanımaktadır [15].

WannaCry, Microsoft Windows'u hedef alan bir fidye virüsüdür. Mayıs 2017'de 99 ülkedeki 230.000 bilgisayara bulaşarak 28 dilde fidye talep eden geniş çaplı bir siber saldırı başlatmıştır. WannaCry, bulaştığı bilgisayardaki dosyaları şifreleyip yeniden erişime açılabilmesi için fidye talep etmektedir [47].

Temel güvenlik açığını gidermeye yönelik bir düzeltme yaması 14 Mart 2017'de yayımlanmış olmasına rağmen, güvenlik güncelleştirmelerinin uygulanmasının gecikmesi bazı kullanıcıları ve kuruluşları savunmasız bırakmıştır [47].

Windows güvenlik açığı bir sıfırıncı gün açığı değil ancak Microsoft'un 14 Mart 2017'de (neredeyse olaydan tam iki ay önce) bir güvenlik yaması hazırladığı bir güvenlik açığıdır. Düzeltme yaması, Windows tarafından kullanılan Sunucu Mesaj Bloğu (SMB) protokolüne yöneliktir. Microsoft ayrıca kullanıcıları eski SMB1 protokolünü kullanmayı bırakmaya ve daha yeni, daha güvenli SMB3 protokolünü kullanmaya teşvik etmektedir. Kuruluşların virüsten etkilenme sebebi bu güvenlik yamasından yoksun olmaları ve bugüne kadar herhangi birinin fidye yazılımı geliştiricileri tarafından hedef alındığına dair hiçbir kanıt olmamasıdır [47].

WannaCry saldırılarından ilk etkilenen ülkeler Şekil 4.6‘da görülebilmektedir.



Şekil 4.6. WannaCry başlangıçta etkilenen ülkeler[47].

Analiz işlemi için istemci bilgisayar olarak kullanılan sanal Windows7 üzerinde agent.py programı açık konumda iken alınmış olan Snapshot çalıştırılır ve analiz süreci başlatılır. Süreç tamamlandığında sanal işletim sistemi otomatik olarak kapatılır ve sürecin analizi yapılarak rapor hazırlanır.

Bir analiz tamamlandığında, oluşturulan rapor dosyaları özel bir dizinde saklanır. Tüm analizler /etc/cuckoo(ServisinÇalıştığıDizin)/storage/analyses/ dizinindeki veritabanında analiz görevini temsil eden artımlı sayısal kimlikten sonra adlandırılan bir alt dizinin altında saklanır [48].

Aşağıda bir analiz dizini yapısı örneği verilmiştir:

|-- analysis.log

|-- binary

|-- dump.pcap

|-- memory.dmp

|-- files

| |-- 1234567890_dropped.exe

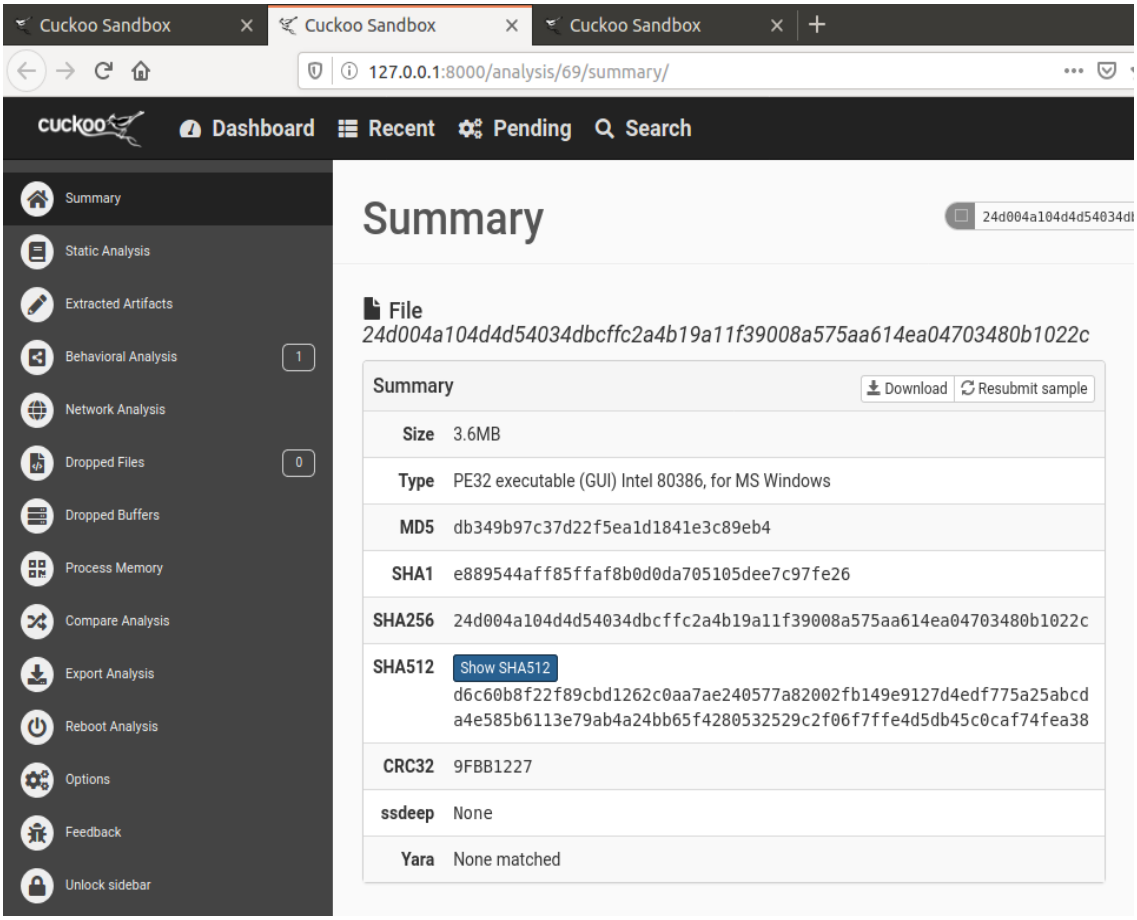
|-- logs

| |-- 1232.bson

```
|   |-- 1540.bson
|   `-- 1118.bson
|-- reports
|   |-- report.html
|   |-- report.json
`-- shots
    |-- 0001.jpg
    |-- 0002.jpg
    |-- 0003.jpg
    `-- 0004.jpg
```

4.2.1. Analiz Özet Bilgileri

Şekil 4.7'de gösterilen analiz raporu özet sekmesinde analiz edilen dosyanın adı, dosya boyutu, MD5, SHA1, SHA256, SHA512, CRC32 hash algoritmalarına göre üretilen değer bilgileri yer alır.



Şekil 4.7. Cuckoo ile Wannacry analizi özet penceresi.

Şekil 4.8'de hash bilgilerinin altında oluşturulan imza bilgileri ve ağ bağlantı özeti yer almaktadır. Wannacry zararlı yazılımının Armadillo v1.71 ile paketlendiği, bilinmeyen bir PE kaynak dosyası adı taşıdığı, GET metodu ile gönderilen http isteğinin url adresinin http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ olduğu görülmektedir.



Şekil 4.8. Cuckoo ile Wannacry analizi http isteği.

İki farklı entropy değeri yüksek sıkıştırılmış veya şifreli dosya bulunmaktadır.

section {u'size_of_data': u'0x0035b000', u'virtual_address': u'0x00310000', u'entropy':

7.99522611944316, u'name': u'.rsrc', u'virtual_size': u'0x0035a454'}

entropy 7.99522611944 Description: A section with a high entropy has been found

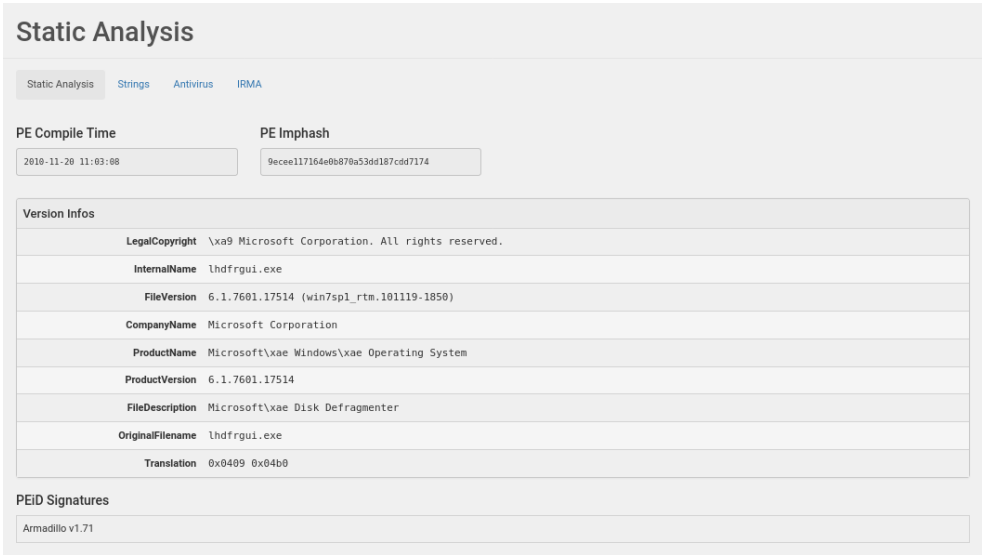
entropy 0.946035242291 Description: Overall entropy of this PE file is high

Hafıza dökümü yapıldığında 404 farklı url bağlantısı yapıldığı ve bu bağlantılardan 50 bağlantının zararlı bağlantı olabilme potansiyeli taşıdığı görülmektedir.

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com adresine yapmış olduğu bağlantı, bağlantının ip adresleri 104.16.173.80, 104.17.244.81 olarak verilmektedir.

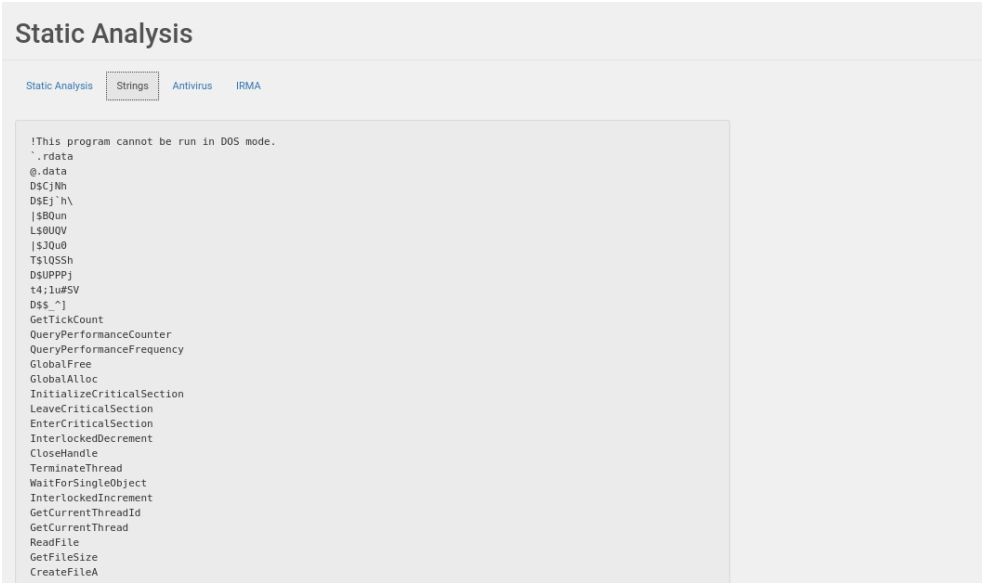
4.2.2. Statik Analiz Bilgileri

Statik analizin temel hedefi, zararlı yazılım hareketlerinin incelenmesinden ziyade, zararlı yazılım hakkında tüm bilgiye sahip olmaktır [49]. Statik analiz bölümünde ise zararlı yazılım çalıştırılmadan alınan bilgiler yer alır. Şekil 4.9'da örnek gösterimi verilen PE dosya formatının nitelikleri ve özellikleri kullanılarak PE başlığında bulunan alanları kullanarak daha anlamlı bilgiler ortaya çıkarmaktadır.



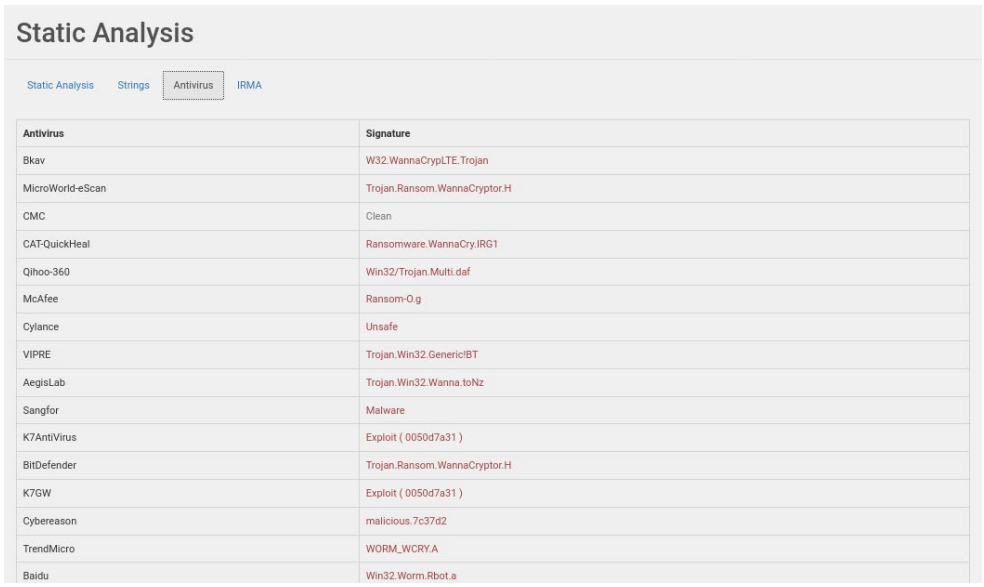
Şekil 4.9. Cuckoo ile Wannacry statik analiz bilgileri.

Statik analiz bölümünde sections, resources ve Imports bilgileri de yer alır. Şekil 4.10'da statik analiz bölümünün Strings sekmesinde analiz edilen yazılım içerisinde geçen anlamlı kelimelerin listesi yer almaktadır.



Şekil 4.10. Cuckoo ile Wannacry statik analizi string bilgileri.

Şekil 4.11'de statik analiz bölümünün Antivirus sekmesinde analiz edilen yazılımın, kötü amaçlı yazılım türlerini tespit etmek için şüpheli dosyaları ve URL'leri analiz eden Virustotal tarafından 60'tan fazla antivirus yazılımı tarafından yapılan analiz sonuç bilgileri verilmektedir.



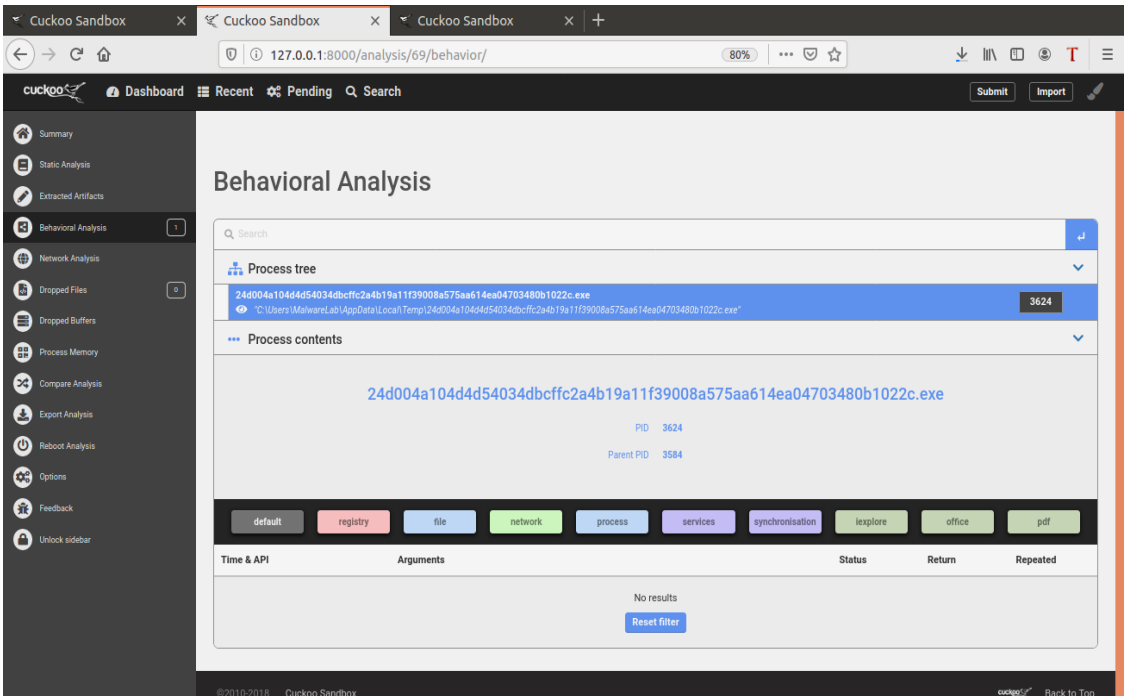
Şekil 4.11. Cuckoo ile Wannacry analizi virustotal sonuçları.

4.2.3. Davranış Analiz Bilgileri

Davranış analizinde, kayıt defteri etkinliği, ağ işlemleri, dosya ve dizin aktarımları gibi kötü amaçlı yazılımların davranışı analiz edilmektedir. Bazen kötü amaçlı yazılım oluştururken yazılımcılar tarafından farkında olmadan hatalar bırakılabilmektedir. Bu

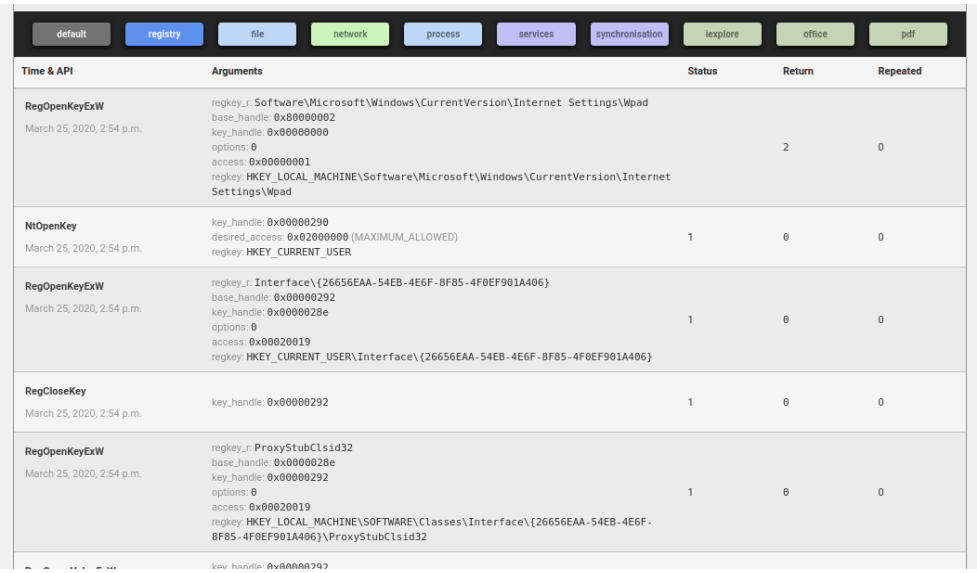
hataların ortaya çıkarılabilmesi işlemi davranış analizi ile yapılabilir. Bu hata bilgileri önemlidir. Bazı durumlarda, hata ayıklama saldırgan hakkında bilgi sağlayabilir. Davranış analizi için İşlem Monitörü, İşlem Gezgini, Regshot, Wireshark, CaptureBat, Cuckoo Sandbox, Anubis, Volatility vb. yaygın olarak kullanılmaktadır [16].

Cuckoo Sandbox Behavioral Analysis bölümünde analiz edilen yazılımın işletim sistemi içerisinde yapmış olduğu davranışsal işlemler ayrıntılı olarak verilmektedir. Şekil 4.12'de örnek gösterimi verilen bu analiz aşamasında yazılımın çalıştığı proses numarasından başlanarak, kayıt defteri(registry) değişiklikleri, ağ bağlantıları, dosya ilişkileri, çalıştırdığı prosesler, servisler, tarayıcı ve pdf bilgileri gibi gerekli tüm davranışsal bilgiler elde edilmektedir.



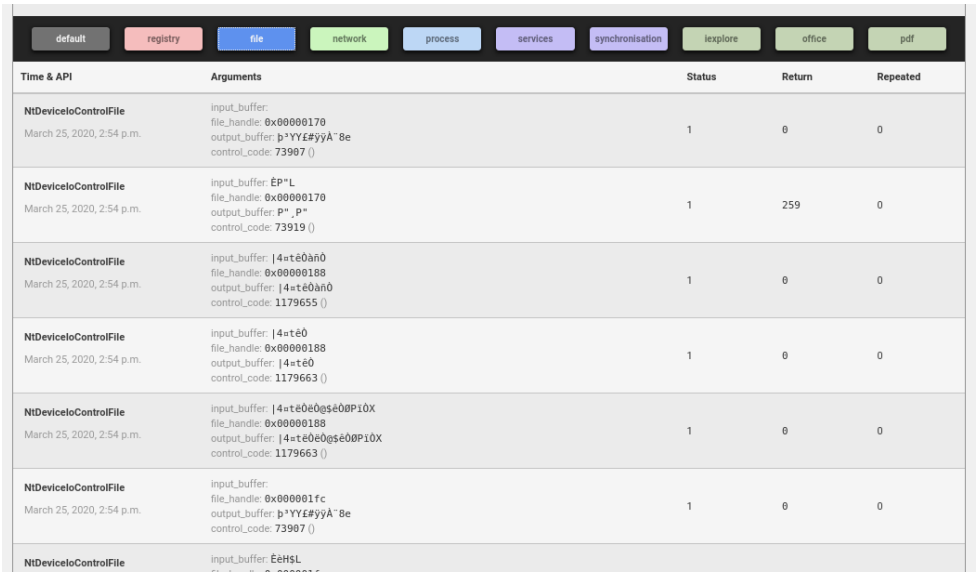
Şekil 4.12. Cuckoo ile Wannacry davranışsal analiz bilgileri.

Şekil 4.13'de behavioral analysis bölümünün registry sekmesinde wannacry yazılımının kayıt defterinden bulunan 76 farklı kayıt üzerinde değişiklik yaptığı belirlenmiştir. Yapmış olduğu kayıt defteri değişikliklerinin tam listesi verilmektedir.



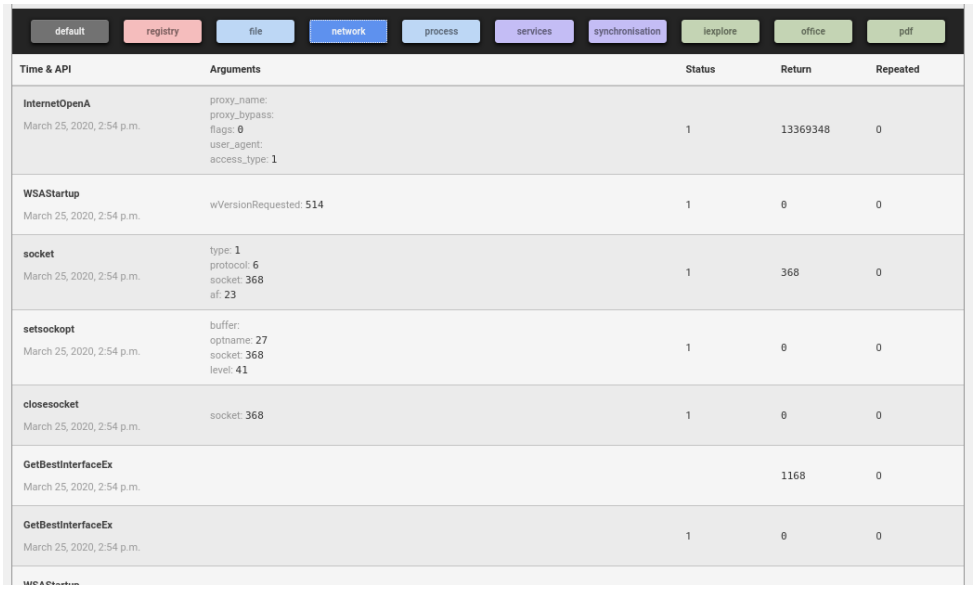
Şekil 4.13. Cuckoo ile Wannacry analizi registry değişiklikleri.

Şekil 4.14'de behavioral analysis bölümünün file sekmesinde wannacry yazılımının 44 farklı dosya işlemi yaptığı belirlenmiştir. Yapmış olduğu dosya işlemlerinin tam listesi verilmektedir.



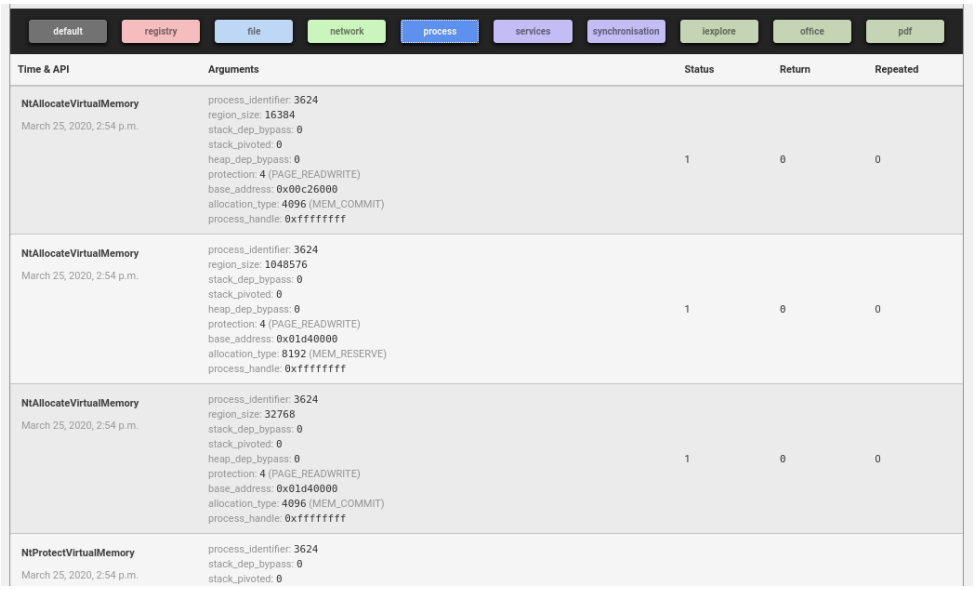
Şekil 4.14. Cuckoo ile Wannacry analizi dosya işlemleri.

Şekil 4.15'de behavioral analysis bölümünün network sekmesinde wannacry yazılımının internet bağlantısı amacıyla yapmış olduğu ağ işlemlerinin tam listesi verilmektedir.



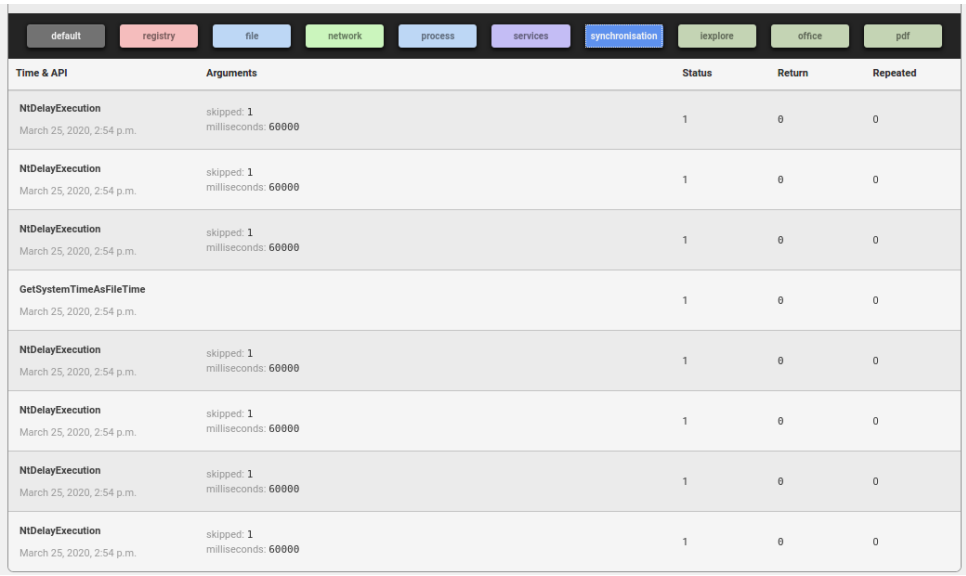
Şekil 4.15. Cuckoo ile Wannacry analizi network işlemleri.

Şekil 4.16'da behavioral analysis bölümünün process sekmesinde wannacry yazılımının 12 farklı process üzerinde değişiklik yaptığı belirlenmiştir. Yapmış olduğu process işlemlerinin tam listesi rapor halinde verilmektedir.



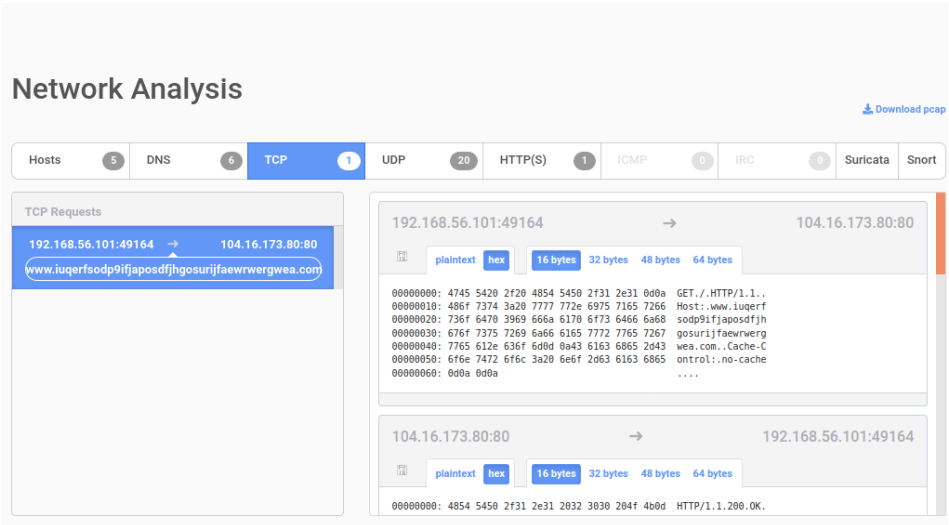
Şekil 4.16. Cuckoo ile Wannacry analizi process işlemleri.

Şekil 4.17'de behavioral analysis bölümünün synchronisation sekmesinde wannacry yazılımının işletim sistemi ile senkronize çalışmak amacıyla yapmış olduğu işlemler listelenir. Bu amaçla işletim sistemi üzerinde 8 farklı işlem belirlenmiştir. Yapmış olduğu işlemlerin tam listesi verilmektedir.



Şekil 4.17. Cuckoo ile Wannacry analizi senkronizasyon işlemleri.

Şekil 4.18'de network analysis bölümünde GET metodu ile yapılan bağlantıların Host bilgileri, DNS, TCP, UDP ve HTTPS bağlantıları hakkında bilgiler verilmektedir. Bu bölümde TCP sekmesinde kaynak-hedef ip adresleri ile kaynak-hedef port numaraları, url adresi bilgileri yer almaktadır. Bu bölümden kurulan ağ bağlantısının pcap dosyası da alınabilmektedir.



Şekil 4.18. Cuckoo ile Wannacry analizi ağ işlemleri.

4.3. CUCKOO SANDBOX İLE PETYA ZARARLI YAZILIM ANALİZİ

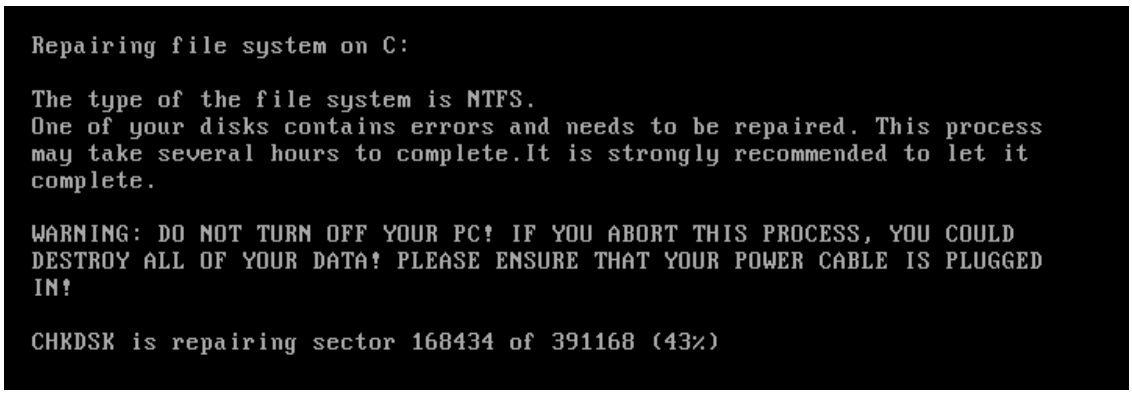
Analiz işlemi, Ubuntu dağıtımına yüklenen Cuckoo Sandbox 2.0.7 servisinin Virtualbox 6.1 üzerinde Windows7 sanal işletim sistemini çalıştırması ile gerçekleştirilmektedir.

Petya zararlı yazılımı, malshare.com üzerinde yapılan tarama ile elde edilmiştir. Elde edilen 26b4699a7b9eeb16e76305d843d4ab05e94d43f3201436927e13b3ebafa90739 isimli yazılım, 127.0.0.1:8000 numaralı localhost portunda çalıştırılan Cuckoo sandbox ile analiz edilmiştir.

Zararlı yazılım, ilk olarak kimlik avı e-postaları aracılığıyla dağıtılır ve fidye yazılımının ağ içinde daha fazla dağıtılması için kötü amaçlı yazılımın kullandığı MS17-10 güvenlik açığı, saldırgan tarafından uzaktan kod yürütülmesine izin vermektedir. Petya, komutları kullanarak Windows Yönetim Araçları'na (WMI) uzaktan erişimi de kullanmaktadır. Ayrıca analizi daha zor hale getirmek için sistem kayıtlarını da temizlemektedir.

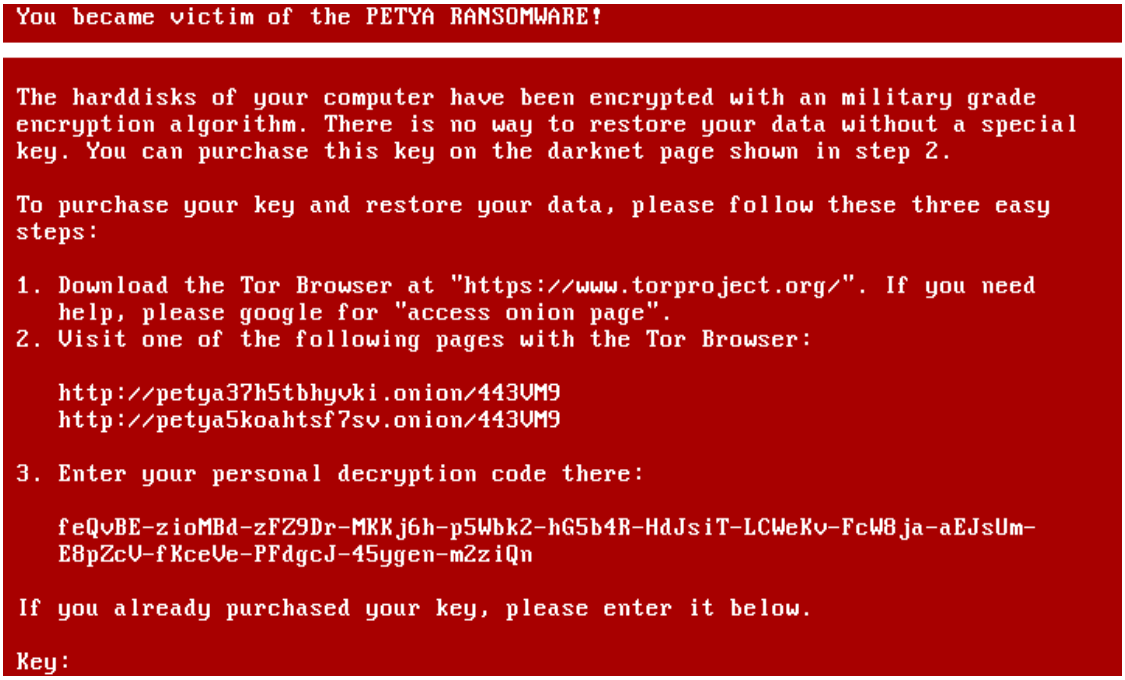
Petya, 2016 yılında ilk kez keşfedilen şifreleme tabanlı bir fidye yazılımı ailesidir [50]. Zararlı yazılım, Microsoft Windows tabanlı sistemleri hedefler ve ana önyükleme kaydını bozarak sabit sürücünün dosya sistemi tablosunu şifreler ve Windows'un ön yüklenmesini önlemektedir. Daha sonra kullanıcının sisteme yeniden erişim sağlamak için Bitcoin olarak ödeme yapmasını talep etmektedir.

Petya zararlı yazılımı bilgisayarın ana önyükleme kaydına bulaşır, Windows önyükleyicisinin üzerine yazar ve işletim sisteminin yeniden başlatılmasını tetikler. Sistem yeniden yüklendiğinde sabit diskin sektörünü onarırken gösterir, ancak tarafta aslında daha sonra dosyalara erişimi reddedecek olan ana önyükleme tablosunu şifrelemektedir [30]. İşletim sistemi yeniden başladığında, bilgisayar ekranında Windows dosya sistemi tarayıcısı Şekil 4.19'da gösterilen chkdsk tarafından üretilen ve sabit sürücünün sektörlerinin onarıldığına işaret edilen metin görüntülenir [50].



Şekil 4.19. Petya chkdsk görünümü.

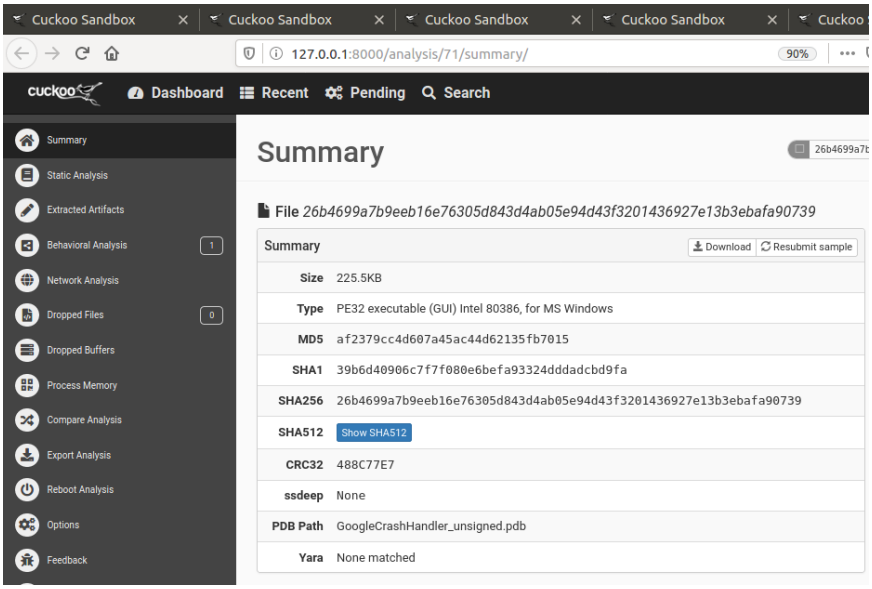
Chkdsk işleminin tamamlanmasının ardından Şekil 4.20'de yer gösterilen kilitleme ve bilgilendirme penceresi gelmektedir.



Şekil 4.20. Petya kilitleme ve bilgilendirme penceresi.

4.3.1. Analiz Özet Bilgileri

Şekil 4.21'de gösterilen analiz raporu özet sekmesinde analiz edilen dosyanın adı, dosya boyutu, MD5, SHA1, SHA256, SHA512, CRC32 hash algoritmalarına göre üretilen değer bilgileri yer almaktadır.



Şekil 4.21. Cuckoo ile Petya analizi özet penceresi.

PDB, bir program (veya genellikle DLL veya EXE gibi program modülleri) hakkında hata ayıklama bilgilerini depolamak için özel bir dosya biçimidir (Microsoft tarafından

geliştirilmiştir). PDB dosyaları genellikle .pdb uzantısına sahiptir. PDB dosyası genellikle derleme sırasında kaynak dosyalardan oluşturulmaktadır. Modüldeki tüm sembollerin bir listesini adresleriyle ve muhtemelen dosyanın adını ve sembolün bildirildiği satırı saklar [51]. GoogleCrashHandler_unsigned.pdb adında pdb vardır.

NtProtectVirtualMemory ve NtAllocateVirtualMemory adında iki olay ile yazılım kendini yükleyebileceği hafıza alanı ayırır.

entropy 7.19364119948 description A section with a high entropy has been found

entropy 0.694877505568 description Overall entropy of this PE file is high

Değeri yüksek olan iki entropy bulundu.

LookupPrivilegeValueW privilege_name: SeShutdownPrivilege

Sistemde şüpheli bir özel bölge için yerel olarak kullanılan benzersiz tanımlayıcı bulunmaktadır.

host 195.175.113.40

host 40.74.35.71

DNS sorgusu olmadan kurmuş olduğu ana bilgisayar bağlantısı bulunmuştur. Harddiske bulaşmak üzere 50 farklı bootkit bulunmuştur. Dosya, Şekil 4.22'de görüldüğü gibi VirusTotal'deki 66 Antivirüs programında 50'si tarafından hangi isimlerle tanındığı bilgileri ile birlikte kötü amaçlı yazılım olarak tanımlanmaktadır.

File has been identified by 66 AntiVirus engines on VirusTotal as malicious (50 out of 66 events)

Bkav	W32.TiposcoAU.Trojan
MicroWorld-eScan	Trojan.Ransom.Petya.C
CMC	Trojan-Ransom.Win32!O
CAT-QuickHeal	Ransom.Petya.S5
McAfee	Generic.yk
Malwarebytes	Ransom.Petya
Zillya	Trojan.Petr.Win32.1
CrowdStrike	win/malicious_confidence_100% (W)
Alibaba	Ransom:Win32/Petya.934c9156
K7GW	Trojan (004e14a51)
K7AntiVirus	Trojan (004e14a51)
TrendMicro	Ransom_PETYA.A
Cyren	W32/Trojan.NREO-5105

Şekil 4.22. Cuckoo ile Petya analizi virustotal sonuçları.

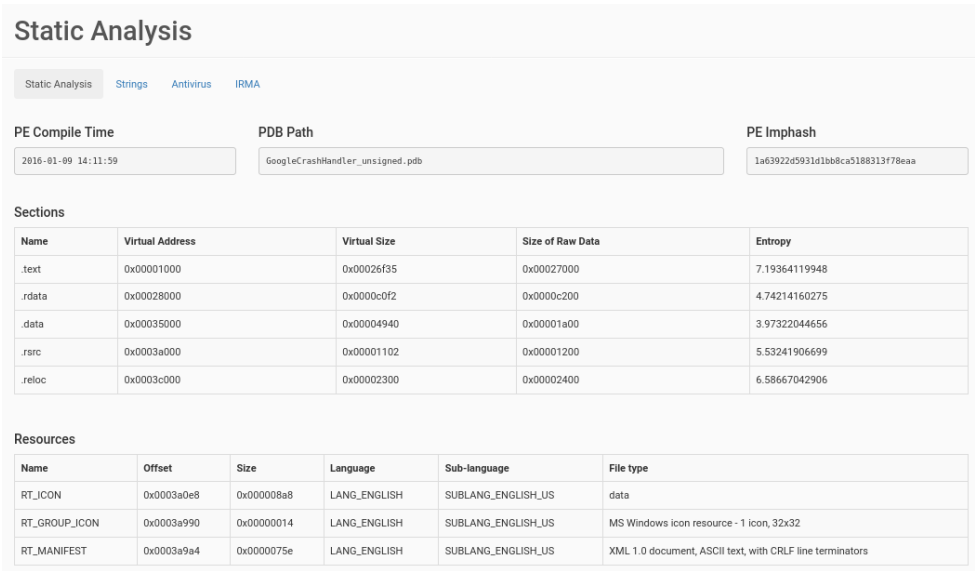
4.3.2. Statik Analiz Bilgileri

Statik analiz bölümünde ise zararlı yazılım çalıştırılmadan alınan bilgiler yer almaktadır. PE dosya formatının yani taşınabilir-çalıştırılabilir dosyaların nitelikleri ve özellikleri kullanılarak PE başlığında bulunan alanları kullanarak daha anlamlı bilgiler ortaya çıkarılabilir.

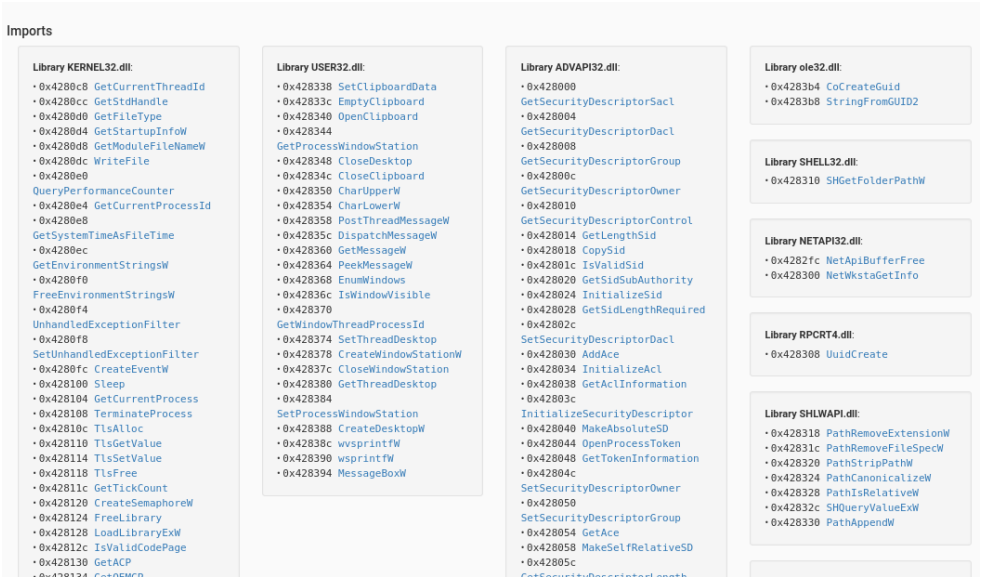
PE Imphash değeri, bir yazılımın (bu durumda arka kapı) diğer dosyalardan (genellikle Windows işletim sistemine işlevsellik sağlayan çeşitli DLL dosyaları) çağırdığı işlevlerin hash değeridir. Yazılımın (bu durumda arka kapı) diğer dosyalardan (genellikle Windows işletim sistemine işlevsellik sağlayan çeşitli DLL dosyaları) çağırdığı işlevlerdir.

PE Sections, çalıştırılabilir dosyanın içerdiği Code, Data gibi bilgileri tutan bölümlerdir. Bu bölümler statik analiz kısmında bulunur [52].

Şekil 4.23'de statik analiz bölümünde sections bilgilerinin yanında dosya kaynak bilgileri resources sekmesinde yer almaktadır. Analiz edilen dosyanın çalıştırılması ile dahil edilen dll dosyaları Şekil 4.24'de imports sekmesinde yer almaktadır.

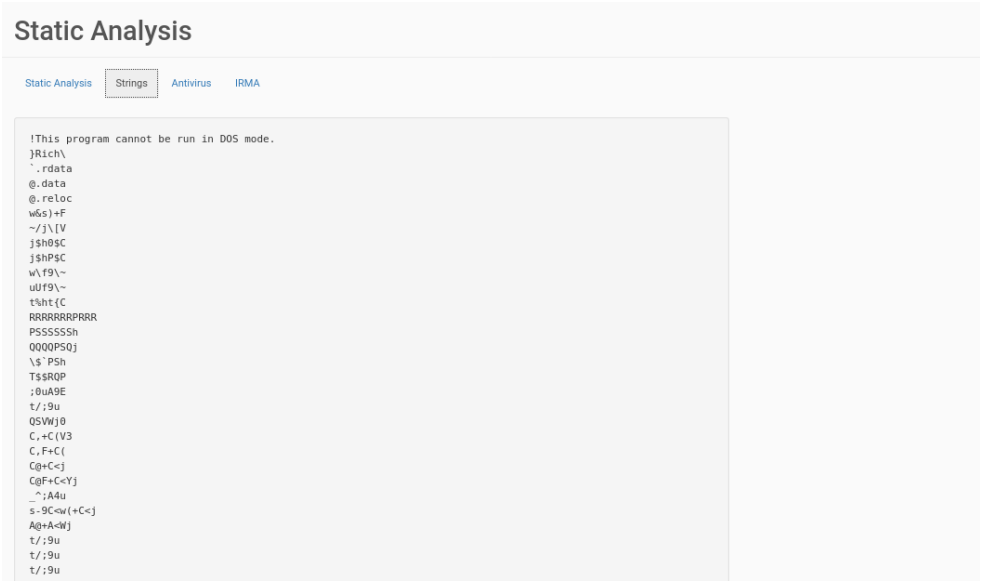


Şekil 4.23. Cuckoo ile Petya statik analiz bilgileri.



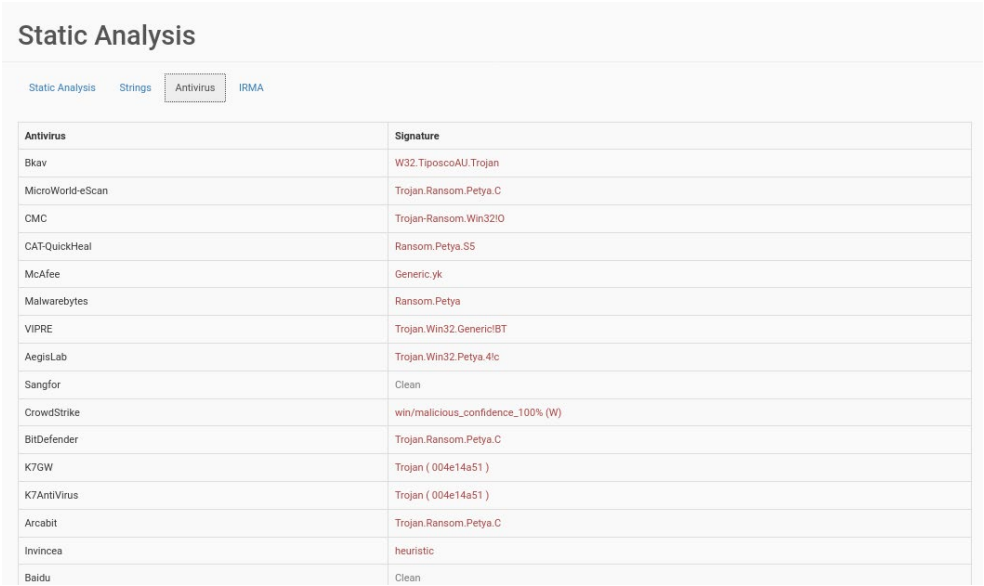
Şekil 4.24. Cuckoo ile Petya dll dosya bilgileri.

Şekil 4.25'de statik analiz bölümünün Strings sekmesinde analiz edilen yazılım içerisinde geçen anlamlı kelimelerin listesi yer almaktadır.



Şekil 4.25. Cuckoo ile Petya statik analizi string bilgileri.

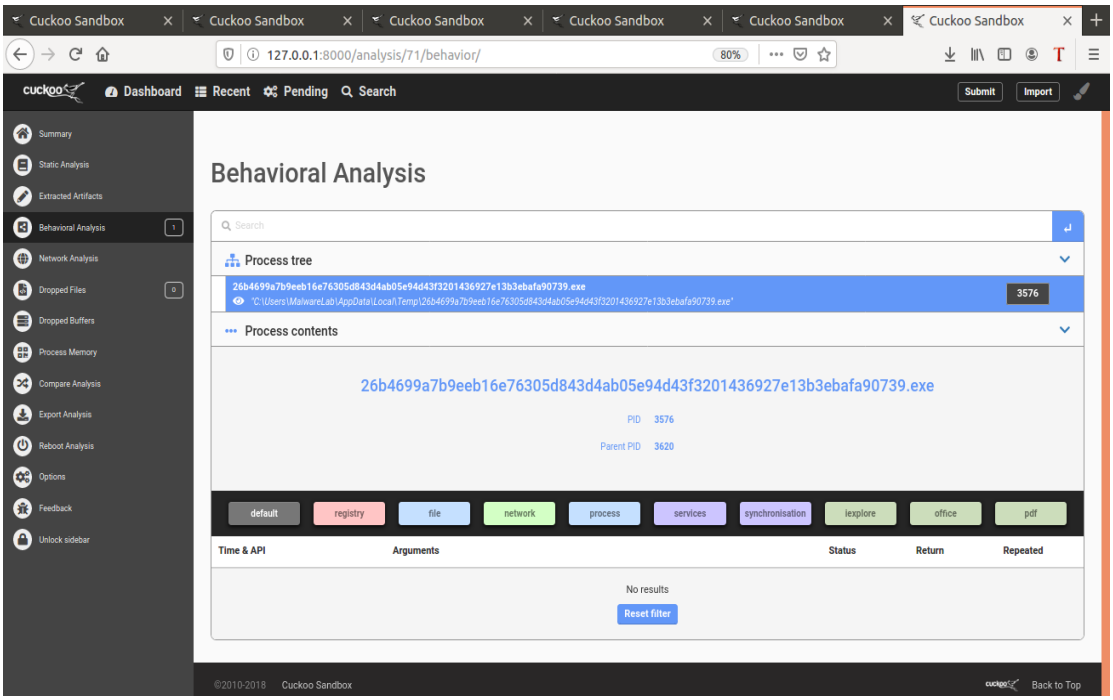
Statik analiz bölümünün Antivirus sekmesinde analiz edilen yazılımın, kötü amaçlı yazılım türlerini tespit etmek için şüpheli dosyaları ve URL'leri analiz eden Virustotal tarafından 60'tan fazla antivirüs yazılımı tarafından yapılan analiz sonuç bilgilerine Şekil 4.26'da yer verilmiştir. Bu bölümde antivirüs yazılımı karşısında imza bilgileri de bulunmaktadır.



Şekil 4.26. Cuckoo ile Petya analizi virustotal sonuçları.

4.3.3. Davranış Analiz Bilgileri

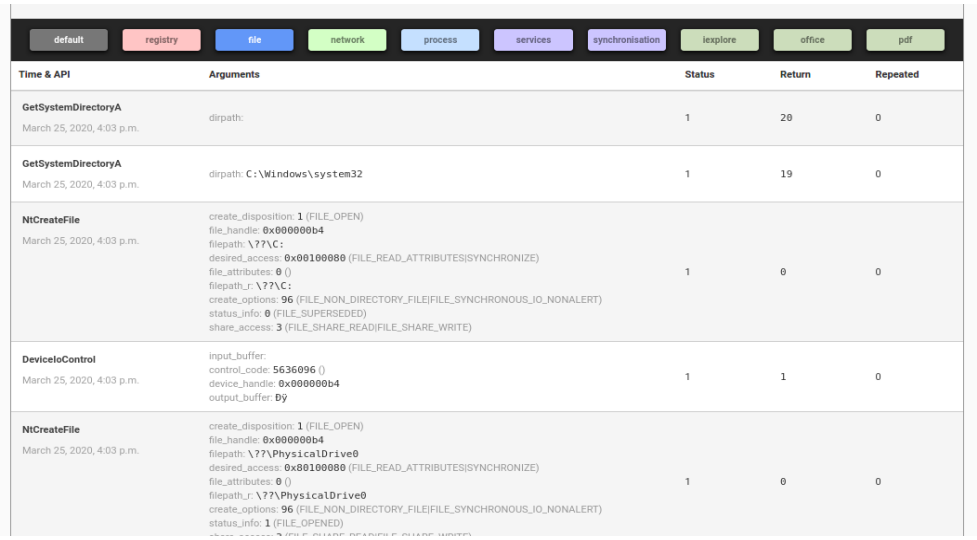
Behavioral analysis bölümünde analiz edilen yazılımın işletim sistemi içerisinde kurmuş olduğu ilişkiler ayrıntılı olarak verilir. Bu analiz aşamasında yazılımın çalıştığı proses numarasından başlanarak, registry değişiklikleri, ağ bağlantıları, dosya ilişkileri, çalıştırdığı prosesler, servisler, tarayıcı ve pdf bilgileri gibi gerekli tüm davranışsal bilgiler elde edilebilmektedir. Şekil 4.27'de örnek gösterime yer verilmiştir.



Şekil 4.27. Cuckoo ile Petya davranışsal analiz bilgileri.

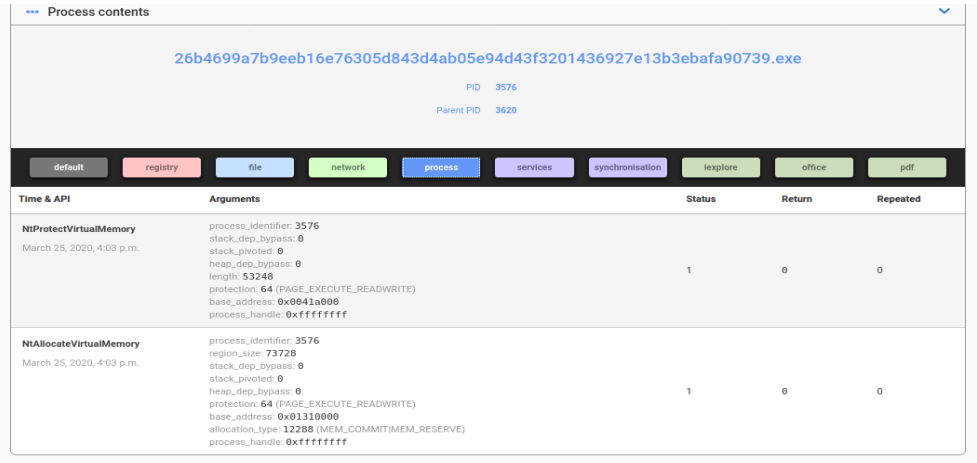
Behavioral analysis bölümünün Petya'nın zararlı yazılımın şifreleme amacıyla harddisk NTFS tablolama bölümünü kullanması nedeniyle registry sekmesinde herhangi bir bilgi bulunamamıştır.

Behavioral analysis bölümünün file sekmesinde Petya yazılımının 27 farklı API üzerinde işlem yaptığı belirlenmiştir. Yapmış olduğu dosya işlemlerinin örneği Şekil 4.28'de verilmektedir. Bu tabloda API adı, çalışma zamanı, API'de kullanılan argümanlar listelenmektedir.



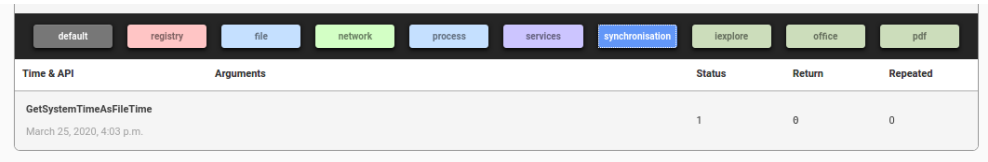
Şekil 4.28. Cuckoo ile Petya analizi dosya işlemleri.

Behavioral analysis bölümünün network sekmesinde petya yazılımının internet bağlantısı amacıyla yapmış olduğu herhangi bir işlem görülememiştir. Analiz aşamasında process sekmesinde yazılımın çalıştığı bellek alanının korunması için iki farklı process başlatıldığı Şekil 4.29'da görülmektedir.



Şekil 4.29. Cuckoo ile Petya analizi process işlemleri.

Behavioral analysis bölümünün services sekmesinde herhangi bir bilgi bulunamamıştır. Synchronisation sekmesinde Petya yazılımının işletim sistemi ile senkronize çalışmak amacıyla bir işlem listelenmektedir. Şekil 4.30'da gösterilen GetSystemTimeAsFileTime ile geçerli sistem tarih ve saatini alır. iexplore, office, pdf sekmelerinde herhangi bir bilgi bulunamamıştır.



Şekil 4.30. Cuckoo ile Petya analizi senkronizasyon işlemleri.

Analiz sonuçlarına göre petya yazılımı özet bölümünden alınan bilgiler, statik analiz bölümünün antivirus sekmesi, davranışsal analiz sekmesinde file, process ve synchronisation sekmesinde alınan bilgilerden yararlanarak yazılımın işletim sistemi için zararlı sonuçlara yol açtığı görülebilmektedir.

5. ZARARLI VE ZARARSIZ YAZILIMLARIN ANALİZ SONUÇLARININ KARŞILAŞTIRILMASI

Sonuçlarını karşılaştırmak amacıyla WannaCry, Petya, Ryuk, Locky, Jigsaw fidye yazılımları ile Putty.exe, MEB_Sertifikası.cer, yazi.txt dosyaları kullanılmıştır. Bu dosyaların Cuckoo Sandbox üzerinde çalıştırılmaları sonucunda ortaya çıkan verilerin analiz edilmesi ile karşılaştırmalar gerçekleştirilmektedir.

Çizelge 5.1'de analiz amacıyla kullanılan dosyaların adları, türleri, MD5 ve CRC32 değerleri verilmektedir. Bu tabloda analizi yapılan tüm dosyalar hakkına ayrıntılı bilgiler bulunmaktadır. Çizelgede yer alan boyut, tür, MD5 ve CRC32 değerleri Cuckoo sandbox özet bilgilerinden alınmıştır.

Çizelge 5.1. Analiz edilen yazılımların genel bilgileri.

No	Kısa Ad	Dosya Uzun Adı	Boyut	Tür	MD5	CRC32
1	Jigsaw	jigsaw.exe	283.5KB	PE32 executable for MS Windows	2773e3dc59472296 cb0024ba7715a64e	3C351D58
2	Wannacry	*24d004a104d4d54 034dbcffc2a4b19a1 1f39008a575aa61 4ea04703480b1022c*	3.6MB	PE32 executable for MS Windows	db349b97c37d22f5 ea1d1841e3c89eb4	9FBB1227
3	Ryuk	fe909d18cf0fde08 9594689f9a69fbc6 d57b69291a09f3b9 df1e9b1fb724222b	152.5KB	PE32+ executable x86-64 for MS Windows	40492c178079e65 dfd5449bf899413b6	6F81D268
4	Locky	2016-10-04-followup-download-Locky.bin.zip	136.0KB	Zip archive data, at least v2.0 to extract	f0b2acf1659d90e 10577d6d125f15cba	7BAE87D5
5	Petya	*26b4699a7b9eeb1 6e76305d843d4ab0 5e94d43f320143692 7e13b3ebafa90739*	225.5KB	PE32 executable for MS Windows	af2379cc4d607a45 ac44d62135fb7015	488C77E7
6	Putty	putty.exe	1.1MB	PE32+ executable for MS Windows	6fa14b3b1c54a26f 0b9bbcd2f6b45899	DA2AB092
7	MEB Sertifika	*MEB_SERTIFIKASI.cer*	899.0B	Data	8d2ef0944d975db f29e31078cec809cd	2CF045DB
8	Pdf Dosya	İşletim Sistemi Kurulumu.pdf	1.3MB	PDF document, version 1.5	bc68c5c3bb20dd5 61b86dfa7930d9a06	C578098E

Çizelge 5.2'de yer alan bilgiler, Cuckoo sandbox özet sekmesinde yer alan bilgilerden yararlanılarak oluşturulmuştur.

Çizelge 5.2. Yazılımların analiz özeti bilgileri.

Kısa Ad	Jigsaw	Wannacry	Ryuk	Locky	Petya	Putty	MEB Sertifika	Pdf Dosya
Bilinmeyen PE dosyası bölümü	2	1				1		
Bootkit oluşturma özelliği					50			
Şifreleme işlemli dosya hareketi				2325				
Virtualbox algılama özelliği				3				
Anahtar dosyası oluşturma				50				
Dns sorgusu				2	2			
User agent ayarlarını okuma				1				
Çalıştırılabilir dosya oluşturma				2				
Ofis dokümanı oluşturma				6				
Debugger kontrolü				1		1		
Bilgisayar adı sorgusu				4				
Kripto anahtarı için kullanılan Mindows api sayısı			50					
Çalıştırılabilir pdb yolu			1		1			
Çalıştırılabilir dosya kısayolu			25					
Potansiyel sandbox kaçınma			44					
Şüpheli ayrıcalık tanıma işlemi			2	2	1			
Çalıştırılabilir dosya sayısı			1					
Farklı bir iş için yürütme izni			10					
Createremotethread ile bir iş parçacığı oluşturma			12				2	
Hafıza manipulasyonu			20					
Dosya uzantısı eklemesi			9	50				
Diske fidye mesajı yazma			50	50				
Şüpheli http trafiği		1		1			2	
Debug edilen process	2						1	
Registry	1						1	
Hafıza üzerinde okuma-yazma-çalıştırma işlemi için yer ayırma	50			50	2			
Veri şifreleme-sıkıştırma işlemi	2	2			2	2		
İşlemci bellek dökümünde potansiyel zararlı url sayısı	50	50				20	50	
Windows başlangıca yüklenme	1							
Virustotal yakalanma oranı	50/67	50/68	50/58	50/55	50/67	0/68	0/68	0/68
Tehlikeli dosya skoru	10	10	8.4	10	10	2	0	0

Sandbox sabit özelliklere bakmak yerine yazılımın dinamik analizini yaparak işletim sisteminde yaptığı değişiklikleri rapor haline getirmesi nedeniyle yazılımların analizi sonucu ortaya çıkan veriler çizelgede farklı satırlarda yer almaktadır. Bu farklılıklara rağmen elde edilen verilerden Jigsaw, Ryuk ve Locky yazılımlarının işletim sistemine verdiği zarar açıkça görülmektedir. Petya yazılımı ile 50 farklı bootkit oluşturması sebebiyle zararlı yazılım olduğu görülmektedir. WannaCry yazılımı ise 50 potansiyel zararlı url bulunmaktadır. Bu verilerin yanında VirusTotal yakalanma oranı ve skor verilerine bakılarak Putty yazılımı dışındaki yazılımların zararlı veya yararlı olduğu görülebilmektedir. Putty yazılımı için yapmış olduğu şifreleme-sıkıştırma işlemi ile potansiyel url bilgileri skor değerini artırmaktadır.

Çizelge 5.3'de Statik analiz sonucu elde edilen veriler yer almaktadır. Bu verilerden 2 yazılımın paketleyici program bilgileri, 1 yazılımın PDB değerinin yanında yazılımların bölüm sayıları, kaynak sayıları ve dahil edilen dosya sayıları elde edilmektedir. Bu verilerin yanında yazılımın zararlı olabilme olasılığına yönelik bilgi ise antivirüs satırında yer alan verilerden elde edilmektedir.

Çizelge 5.3. Yazılımların statik analiz bilgileri.

Kısa Ad	Jigsaw	Wannacry	Ryuk	Locky	Petya	Putty	MEB Sertifika	Pdf Dosya
PE Compile Time	31.03.2016 09:28:14	2010.11.20 11:03:08	2018.12.21 03:15:31	4.10.2016 22:59:32	2016.01.09 14:11:59	2019.09.22 12:28:30	-	-
PE Imphash	f34d5f2d 4577ed6d 9ceec516 c1f5a744	9ecee117 164e0b87 0a53dd18 7cdd7174	c7a0309d 45fd007c 2ce268b7 218e075c	eadb9952 7332f2bc 7e9fd730 aad84b65	1a63922d 5931d1bb 8ca51883 13f78eaa	2e3215ac c61253e5 fa73a840 384e9720	-	-
PEiD Signatures		Armadillo v1.71		PureBasic 4.x			-	-
PDB Path			1				-	-
Bölümler (Sections)	5	4	7	5	5	8	-	-
Kaynaklar (Resources)	2	2	1	1	3	22	-	-
Dahil Edilenler (Imports)	1	7	3	5	10	8	-	-
Antivirüs	67/72	68/73	58/73	55/67	67/73	0/71	-	-

Çizelge 5.4'de yer alan veriler ile yazılımların çalışması esnasında işletim sistemi

üzerinde yapmış oldukları davranışsal değişiklikler yer almıştır. Zararlı yazılımların dosya hareketinin daha fazla olduğu görülmektedir.

Çizelge 5.4. Yazılımların davranışsal analiz bilgileri.

Kısa Ad	Jigsaw	Wannacry	Ryuk	Locky	Petya	Putty	MEB Sertifika	Pdf Dosya
Registry	476	63	10	100+		100+	100+	
File	131	1	100+	100+	100+	4	20	1
Network		5	100+	9		1		
Process	410	25	173	100+	2	89	17	1
Services		4	10					
Synchronisation	26	1	20		1	10	1	1

Çizelge 5.5'de yazılımların ağ hareketleri görülmektedir. Ağ hareketleri incelendiğinde bazı yazılımların faydalı bağlantılar gerçekleştirirken Jigsaw, Wannacry, Ryuk, Locky yazılımlarının bilinmeyen zararlı olabilecek ip adreslerine istek gerçekleştirdiği görülmüştür. Petya yazılımının ise zararlı bir fidye yazılımı olmasına rağmen herhangi bir bağlantı ağ bağlantısı belirlenememiştir. Buradan çıkarılan sonuç ile network tabanlı yapılan bir analizin tek başına doğru sonuçlar ortaya koymadığı görülmektedir.

Çizelge 5.5. Yazılımların ağ hareket bilgileri.

Kısa Ad	Jigsaw	Wannacry	Ryuk	Locky	Petya	Putty	MEB Sertifika	Pdf Dosya
HOST	2	2	2	4	0	2	3	0
DNS	4	4	4	14	3	4	5	0
TCP	0	1	0	1	0	0	1	0
UDP	18	12	18	27	9	11	16	0
HTTP	0	0	0	0	0	0	0	0
HTTPS	0	1	0	1	0	0	1	0
ICMP	1	0	1	2	0	0	1	0

6. SONUÇLAR VE ÖNERİLER

Bu yüksek lisans tezinde, her geçen gün yaygınlaşan ve ciddi mali kayıplara neden olan fidye yazılımlarının analizi üzerine çalışma yapılmıştır. Bu çalışma ile fidye yazılımlarının yapısını analiz etmek amacıyla deneysel analiz ortamı hazırlanmıştır. Hazırlanan analiz ortamında güvenlik duvarı yapısı aracılığıyla tüm ağ hareketlerinin, kum havuzu yapısı ile çalıştırıldığı işletim sistemi üzerindeki dinamik hareketlerin analiz edilmesi amaçlanmıştır.

Literatür araştırmasında fidye yazılımlarının dünya genelinde vermiş olduğu zararın her geçen gün arttığı görülmüştür. Siber saldırganlar için kolay para kazanma yöntemi olması sebebiyle alınan önlemler karşısında fidye yazılımlarının da kendini her geçen gün geliştirmektedir. Bireysel kullanıcıların ve kurumların zararlı yazılımlar ve internetin güvenli kullanımı konusunda bilinçlendirilmesi önem kazandığı görülmektedir.

Bu çalışmada, online sistemlere ihtiyaç duyulmadan kurumların kendi bünyelerinde yapılandırabileceği deneysel analiz ortamı önerilmiştir. Kurulan analiz ortamında zararlı ve zararsız yazılımların analizi yapılarak ortaya çıkan sonuçlar ile yazılımların işletim sistemine etkileri analiz edilmiştir. Ağ tabanlı analiz ile kum havuzu üzerinde yapılan davranışsal analizin birleştirilmesinin daha doğru ve etkili sonuçlar ortaya çıkardığı görülmüştür.

Bu çalışma esas alınarak küçük ölçekli kurumların ve araştırmacıların kullanabileceği çalışma ortamları geliştirilebilir. Bu çalışmada analiz öncesi istemci bilgisayarlar üzerindeki güvenlik açıkları göz ardı edilmiştir.

Bu tez çalışmasında remnux işletim sistemi ile elde edilen ağ hareketi bilgileri ile Cuckoo sandbox içerisinde veritabanında tutulan ağ hareketlerinin birleştirilmesi ile ileride yapılacak çalışmalara altyapı olabilecek veri kümesi elde edilebilmektedir. Bu bilgiler ve elde edilebilecek veri kümesi ile makine öğrenmesi yöntemleri kullanılarak fidye yazılımlarını önleyecek araçlar geliştirilebilir.

7. KAYNAKLAR

[1] S. Saxena, "Prevention", *Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, ss. 1–4, 2018.

[2] D. F. Netto, K. M. Shony, ve E. R. Lalson, "An Integrated Approach for Detecting Ransomware Using Static and Dynamic Analysis", 2018 International CET Conference on Control, Communication, and Computing, IC4 2018, ss. 410–414, 2018.

[3] Anonim, (May. 13, 2020). "2020 Türkiye İnternet Kullanımı ve Sosyal Medya İstatistikleri". [Online].Erişim: https://dijilopedi.com/2020-turkiye-internet-kullanimi-ve-sosyal-medya-istatistikleri/

[4] P. O'Kane, S. Sezer, ve D. Carlin, "Evolution of ransomware", *IET Networks,* c. 7, sayı 5, ss. 1–7, 2018.

[5] İ. Kara, "Üçüncü Nesil Cerber Ransomware Zararlı Yazılımının Statik ve Dinamik Analizi Static and Dynamic Analysis of Third Generation Cerber Ransomware", ss. 3–4, 2018.

[6] J. S. Aidan, Zeenia, ve U. Garg, "Advanced Petya Ransomware and Mitigation Strategies", ICSCCC 2018 - 1st International Conference on Secure Cyber Computing and Communications, ss. 23–28, 2018.

[7] E. Berrueta, D. Morato, E. Magana, ve M. Izal, "A Survey on Detection Techniques for Cryptographic Ransomware", *IEEE Access,* c. 7, ss. 144925–144944, 2019.

[8] A. Fagioli, "Zero-day recovery: the key to mitigating the ransomware threat", Computer Fraud and Security, c. 2019, sayı 1, ss. 6–9, 2019.

[9] Anomim, (May. 13, 2020). "Remnux Linux Dağıtımının İncelenmesi ve Örnek bir Kötücül Yazılım Analiz Uygulaması. Review of Remnux Linux Distro and a Sample Malware Analysis - PDF Free Download". [Online].Erişim: http://docplayer.biz.tr/52325140-Remnux-linux-dagitiminin-incelenmesi-ve-ornek-bir-kotucul-yazilim-analiz-uygulamasi-review-of-remnux-linux-distro-and-a-sample-malware-analysis.html

[10] D. Min vd., "Amoeba: An Autonomous Backup and Recovery SSD for Ransomware Attack Defense", *IEEE Computer Architecture Letters,* c. 17, sayı 2, ss. 243–246, 2018.

[11] S. Sheen ve A. Yadav, "Ransomware detection by mining API call usage", 2018 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2018, ss. 983–987, 2018.

[12] İ. Kara, "Analysis Techniques of Web Based Malware and Attack Methods", sayı 1, ss. 46–53.

[13] A. O. Almashhadani, M. Kaiiali, S. Sezer, ve P. O'Kane, "A Multi-Classifier

Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware", *IEEE Access,* c. 7, ss. 47053–47067, 2019.

[14] R. Agrawal, J. W. Stokes, K. Selvaraj, ve M. Marinescu, "University of California, Santa Cruz , Santa Cruz , CA 95064 USA Microsoft Corporation, One Microsoft Way , Redmond , WA 98052 USA", ss. 3222–3226, 2019.

[15] M. Akbanov, V. G. Vassilakis, ve M. D. Logothetis, "Ransomware detection and mitigation using software-defined networking: The case of WannaCry", Computers and Electrical Engineering, c. 76, ss. 111–121, 2019.

[16] I. Kara, "A basic malware analysis method", *Computer Fraud and Security,* c. 2019, sayı 6, ss. 11–19, 2019.

[17] S. R. Davies, R. Macfarlane, ve W. J. Buchanan, "Forensic Science International : Digital Investigation Evaluation of live forensic techniques in ransomware attack mitigation", *Forensic Science International: Digital Investigation*, c. 33, s. 300979, 2020.

[18] S. H. Kok, A. Abdullah, ve N. Z. Jhanjhi, "Journal of King Saud University – Computer and In- formation Sciences Early detection of crypto-ransomware using pre-encryption detection algorithm", *Journal of King Saud University - Computer and Information Sciences,* 2020, doi: 10.1016/j.jksuci.2020.06.012.

[19] M. Humayun, N. Z. Jhanjhi, A. Alsayat, ve V. Ponnusamy, "Internet of things and ransomware : Evolution , mitigation and prevention", *Egyptian Informatics Journal*, 2020, doi: 10.1016/j.eij.2020.05.003.

[20] A. Arabo, R. Dijoux, T. Poulain, ve G. Chevalier, "ScienceDirect ScienceDirect ScienceDirect Detecting Ransomware Using Process Behavior Analysis Detecting Ransomware Using Process Behavior Analysis", *Procedia Computer Science,* c. 168, sayı 2019, ss. 289–296, 2020.

[21] A. Patel ve J. Tailor, "A malicious activity monitoring mechanism to detect and prevent ransomware", *Computer Fraud & Security Bulletin,* sayı 1, ss. 14–19, 2020.

[22] A. Koltuksuz, "Imaging and evaluating the memory access for malware", *Forensic Science International : Digital Investigation*, 2020, doi: 10.1016/j.fsidi.2019.200903.

[23] S. Rizvi, R. J. Orr, A. Cox, P. Ashokkumar, ve M. R. Rizvi, "Identifying the attack surface for IoT network", *Identifying the attack surface for IoT network* , c. 9, ss. 1–20, 2020

[24] A. Baldin, "Best practices for fighting the fileless threat", *Network Security*, c. 2019, sayı 9, ss. 13–15, 2019.

[25] S. Lee, H. K. Kim, ve K. Kim, "Ransomware protection using the moving target defense perspective", *Computers and Electrical Engineering,* c. 78, ss. 288–299, 2019, doi: 10.1016/j.compeleceng.2019.07.014.

[26] İ.Kara, "Teslacrypt Fidye Yazilim Virüsünü Tespiti, Teknik ve Çözümü", *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi,* c. 2, sayı 2, ss. 87–94, 2018.

[27] Anonim, (May. 13, 2020). "Şifreleme Yöntemleri". [Online].Erişim: https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ şifreleme-yöntemleri

[28] Anonim, (May. 13, 2020). “Derin Ağ - Vikipedi”. [Online].Erişim: https://tr.wikipedia.org/wiki/Derin_Ağ

[29] Anonim, (May. 13, 2020). “Fidye Ödemeyin: NoMoreRansom.org”. [Online].Erişim: https://bilimgenc.tubitak.gov.tr/makale/fidye-odemeyin-nomoreransomorg

[30] J. S. Aidan, H. K. Verma, ve L. K. Awasthi, “Comprehensive survey on petya ransomware attack”, Proceedings - 2017 International Conference on Next Generation Computing and Information Systems, ICNGCIS 2017, 2018, doi: 10.1109/ICNGCIS.2017.30.

[31] Anonim, (May. 13, 2020). “Ransomware - Wikipedia”. [Online].Erişim: https://en.wikipedia.org/wiki/Ransomware

[32] M.B.Şentürk, (May. 13, 2020). “Fidye Yazılımlarının Tarihçesi ve Türleri”. [Online].Erişim: https://www.mburaks.com/fidye-yazilimlarinin-tarihcesi-ve-turleri/

[33] D. Su, J. Liu, X. Wang, ve W. Wang, “Detecting Android Locker-Ransomware on Chinese Social Networks”, *IEEE Access,* c. 7, ss. 20381–20393, 2019.

[34] M. Akbanov, V. G. Vassilakis, ve M. D. Logothetis, “WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms”, *Journal of Telecommunications and Information Technology,* sayı 1, ss. 113–124, 2019.

[35] Anonim, (May. 13, 2020). “Racketeer/Crypt0L0cker: Fidye Zararlısı”. [Online].Erişim: https://trapmine.com/blog/racketeer-crypt0l0cker-fidye-zararlisi/

[36] O.Morelli, (May. 13, 2020). “How to identify an email infected with a virus?”. [Online].Erişim: https://www.2-spyware.com/how-to-identify-an-email-infected-with-a-virus

[37] M.Kaya, (May. 13, 2020). “PTT Kargo Takip Virüsü – Malware/Ransomware/CryptoLocker – ptt-tracking.net – ptt.posta.biz”. [Online].Erişim: https://www.muratkaya.com.tr/2015/03/10/ptt-kargo-takip-virusu-malwareransomwarecryptolocker-ptt-tracking-net-ptt-posta-biz/

[38] Anonim, (May. 13, 2020). “Yeni CryptoLocker Virüsü” [Online].Erişim: https://www.4gen.net/yeni-cryptolocker-virusu/

[39] B. Maschinen, A. Investition, G. Beschaffungen, B. Ersatzbeschaffungen ve S. Mittelherkunft, “Information Technology Security Infrastructure Malware Detector System”, *International Journal of Advanced Trends in Computer Science and Engineering,* doi: 10.30534/ijatcse/2020/103922020

[40] Anonim, (May. 13, 2020). “Oracle VirtualBox 6.1 Released as New Major Update”. [Online].Erişim: http://ubuntuhandbook.org/index.php/2019/12/oracle-virtualbox-6-1-released/

[41] Anonim, (May. 13, 2020). “Adli Bilişim İncelemelerinde YARA İle Zararlı Kod Tespiti”. [Online].Erişim: http://halilozturkci.com/adli-bilisim-incelemelerinde-yara-ile-zararli-kod-tespiti/

[42] Anonim, (May. 13, 2020). “Python Imaging Library”. [Online].Erişim: https://tr.wikipedia.org/wiki/Python_Imaging_Library

[43] Anonim, (May. 13, 2020). “How to detect the presence of Wannacry Ransomware

and SMBv1". [Online].Erişim: https://www.netfort.com/blog/detect-wannacry-ransomware/

[44] Anonim, (May. 13, 2020). "Wireshark Nedir? Nasıl Kullanılır?". [Online].Erişim: https://www.karel.com.tr/bilgi/wireshark-nedir-nasil-kullanilir

[45] Anonim, (May. 13, 2020). "Wireshark". [Online].Erişim: https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/wireshark (erişim May. 13, 2020).

[46] A.Chuquilla, T.Guarda ve G.N.Quina "Ransomware – WannaCry", 2019 14th Iberian Conference on Information Systems and Technologies (CISTI) 19 – 22 June 2019.

[47] Anonim, (May. 13, 2020). "WannaCry". [Online].Erişim: https://tr.wikipedia.org/wiki/WannaCry

[48] Anonim, (May. 13, 2020). "Analysis Results — Cuckoo Sandbox v2.0.6 Book". [Online].Erişim: https://cuckoo.readthedocs.io/en/latest/usage/results/

[49] İ.Kara, "Türkiye'de Zararlı Yazılımlarla Mücadelenin Uygulama Ve Hukuki Boyutunun Değerlendirilmesi", *Akademik Bakış Dergisi,* Sayı: 52, Kasım – Aralık 2015

[50] Anonim, (May. 13, 2020). "Petya (malware)". [Online].Erişim: https://en.wikipedia.org/wiki/Petya_(malware)

[51] Anonim, (May. 13, 2020). "Program database". [Online].Erişim: https://en.m.wikipedia.org/wiki/Program _database

[52] Anonim, (May. 13, 2020). "Zararlı Yazılım Analizi – 2 | Statik Analiz". [Online].Erişim: https://www.sibertalimhane.com/zararli-yazilim-analizi/zararli-yazilim-analizi-2-statik-analiz/

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Bahattin DOĞAN

Doğum Tarihi ve Yeri : 26/01/1979 - Oberhausen / ALMANYA

Yabancı Dili : İngilizce

E-posta : bahattindogan@gmail.com

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Lisans	Bilgisayar Mühendisliği	Karabük Üniversitesi	2016
Lisans	Bilgisayar Sistemleri Öğretmenliği	Gazi Üniversitesi	1999
Lise		Fener Lisesi	1995

YAYINLAR

1. **Doğan B**, Kara R, Çetiner E, **"**Preparing Experimental Environment For The Analysis Of Malicious Softwares", 7th Internationa"l Congress on Fundamental and Applied Sciences 2020 (ICFAS2020), October 2020, Prishtina, Kosovo.