

Kötü Amaçlı Yazılım ve Kötü Amaçlı Yazılım Türleri

Kötü amaçlı yazılım, MALicious SofWARE kelimelerinden türetilmiş bir kelimedir. Sistemin bütünlüğüne ve güvenliğine zarar verecek kötü niyetli bir amacı hedefleyen yazılımlara kötü amaçlı yazılım denir.

Günümüzde siber tehdit aktörleri karmaşık kötü amaçlı yazılımlar kullanıyor. Bu tür kötü amaçlı yazılımlar, analizi zorlaştıran teknikler içerir.

Kötü Amaçlı Yazılım Türleri

Kötü amaçlı yazılımlar, özelliklerine/davranışlarına göre birçok türe ayrılmaktadır. Analiz sonucunda, kötü amaçlı yazılımın yetenekleri dikkate alınarak kötü amaçlı yazılımın türü belirlenir.

Bazı kötü amaçlı yazılım türleri ve açıklamaları aşağıdadır:

- **Backdoor:** Kötü amaçlı yazılımın yükleniği cihazda bir arka kapı bırakarak saldırganın bu arka kapı üzerinden sisteme erişmesini sağlar. Örneğin, Shell'e bağlı bir ağ bağlantı noktası açarak saldırganın bu bağlantı noktası üzerinden sisteme bağlanmasını sağlar.
- **Reklam Yazılımı:** Genellikle indirilen yazılımlarla birlikte gelir ve cihazda istenmeyen reklamların görüntülenmesine neden olur. Tüm reklam yazılımları zararlı olmasa da, bazıları varsayılan arama motorunu değiştirir.

- **Ransomware:** Son birkaç yıldır dünya gündeminde olan bir malware türündür. Cihazdaki tüm dosyaları şifreleyerek ve sızdırarak insanlardan fidye talep eder.
- **Virüs:** Vahşi doğada görülen ilk kötü amaçlı yazılım türlerinden biridir. Dolayısıyla günlük hayatı kötü amaçlı yazılım terimi yerine genellikle virüs olarak adlandırıldığını görüyoruz. Virüslerin kendi kendini kopyalama özelliği vardır. Cihazdaki diğer dosyalara bulaşarak kalıcılık sağlar.
- **Solucan:** Bu tür kötü amaçlı yazılımlar, virüslü cihazlardan diğer cihazlara yayıldığından solucan olarak adlandırılır. MS17-010 güvenlik açığından yararlanan bir solucan kötü amaçlı yazılımı olan WannaCry, dünya çapında paniğe neden oldu.
- **Rootkit:** Cihaz üzerinde üst düzey bir yetkiye erişim sağlayarak kendini gizleyen kötü amaçlı yazılım türündür.
- **RAT (Uzaktan Erişim Truva Atı):** Tehdit aktörüne cihaz üzerinde tam kontrol sağlayan bir kötü amaçlı yazılım türündür.
- **Bankacılık kötü amaçlı yazılımları:** Bankacılık uygulamalarını hedef alan ve kurbandan para çalınmasına neden olan bir tür kötü amaçlı yazılım.

Kötü amaçlı yazılım birden fazla özellik içerebilir, bu nedenle kötü amaçlı yazılım birden fazla türe ait olabilir. Örneğin, WannaCry kötü amaçlı yazılımı hem solucan hem de fidye yazılımı kötü amaçlı yazılım özelliklerini içerir.

Kötü Amaçlı Yazılım Analizi İçin Sanal Makine Oluşturma

Sanal makineler

Tüm kişisel dosyalarımızın ve verilerimizin depolandığı cihazda kötü amaçlı yazılımları analiz etmek istemezsiniz. Bu nedenle, kötü amaçlı yazılım analizi için izole cihazlara ihtiyacımız var.

Sanallaştırma yazılımlarını kullanarak kendi cihazınıza sanal işletim sistemi kurabilirsiniz. Bu sayede fiziksel bir cihaz satın almaya gerek kalmadan izole sisteminizi oluşturabilirsiniz.

Ücretli veya ücretsiz olarak kullanabileceğiniz birkaç sanallaştırma ortamı vardır. Bunların en popülerleri VMware'den **VMware Workstation** ve Oracle firmasından **VirtualBox'tır**. Her iki sanallaştırma yazılımı da kötü amaçlı yazılımları analiz etme ihtiyaçlarınızı karşılayacaktır.

Sanallaştırma yazılımlarını kullanmanın bazı dezavantajları vardır.

- Kuracağınız sanal işletim sistemi, ana işletim sisteminizde çalıştığı için fiziksel bir bilgisayar kadar iyi çalışmamayacaktır.
- Sanallaştırma yazılımları da birer yazılım olduğu için bu yazılımlarda zafiyetler oluşabilmektedir. Bu güvenlik açıklarından yararlanan bir kötü amaçlı yazılım sanal ortamdan kaçabilir ve ana işletim sisteminize bulaşabilir. Bu nedenle sanallaştırma yazılımınızı sürekli güncel tutmak isteyebilirsiniz!
- Sanallaştırma yazılımlarının çalışabilmesi için sanal işletim sistemlerine kendi sürücülerini kurması ve çeşitli konfigürasyon dosyaları/kayıtları oluşturması gerekmektedir. Kötü amaçlı yazılım, bu tür göstergeleri kontrol ederek ve sanal bir ortamda çalışıp çalışmadığını kontrol ederek analizi zorlaştıracaktır.

Bu eğitimde **VMware Workstation** ürününü kullanacağız. Bazı özellikler farklılık gösterebilir.

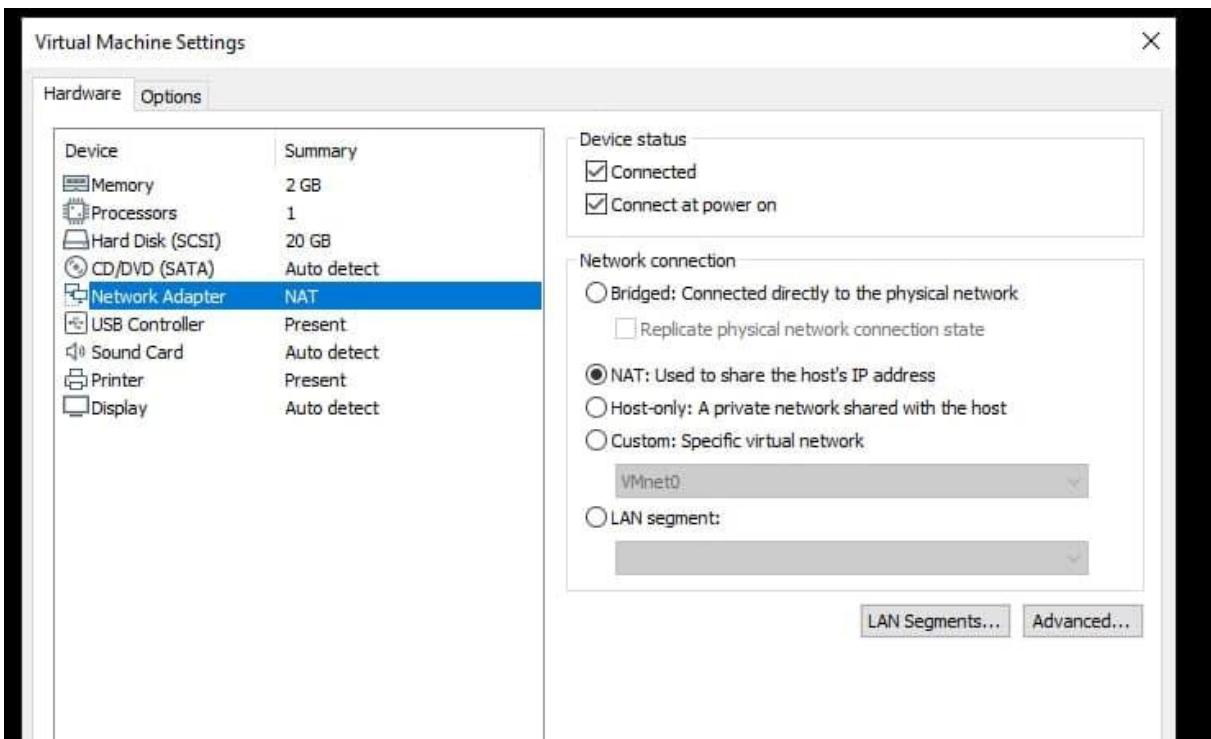
Sanal Makineyi Ayarlama

Sanal işletim sistemini kötü amaçlı yazılım analizine uygun hale getirmelisiniz, aksi takdirde kötü amaçlı yazılım aynı ağdaki diğer cihazlara bulaşabilir.

1) Ağ Ayarları

Analiz edeceğimiz zararlı yazılımların ağ üzerindeki diğer cihazlara bulaşmasını engellemek için kurduğumuz işletim sisteminin ağ ayarlarını

sanallaştırma yazılımından değiştirmeliyiz. Ayarlar kısmından " Network " ayarlarına girmemiz ve burada " Custom " seçeneğini seçmemiz gerekiyor.



- **NAT:** Fiziksel cihazınızın ağ arayüzü üzerinden Internet'e erişmenizi sağlar.
- **Bridge:** Fiziksel cihazınız gibi modeminizden kendi IP adresini alarak internele erişmenizi sağlar.
- **Custom:** Sanallaştırma ortamının oluşturduğu özel ağa dahildir. Bu seçenekte internet erişimi mevcut değildir.

Çalıştıracağımız kötü amaçlı yazılımların ağdaki diğer cihazlara yayılmasını önlemek için sanal işletim sistemimizin ağ erişimini kısıtlamalıyız, bu yüzden " Custom " seçeneğini seçmeliyiz.

2) Anti-Virüs Yazılımını Devre Dışı Bırakın

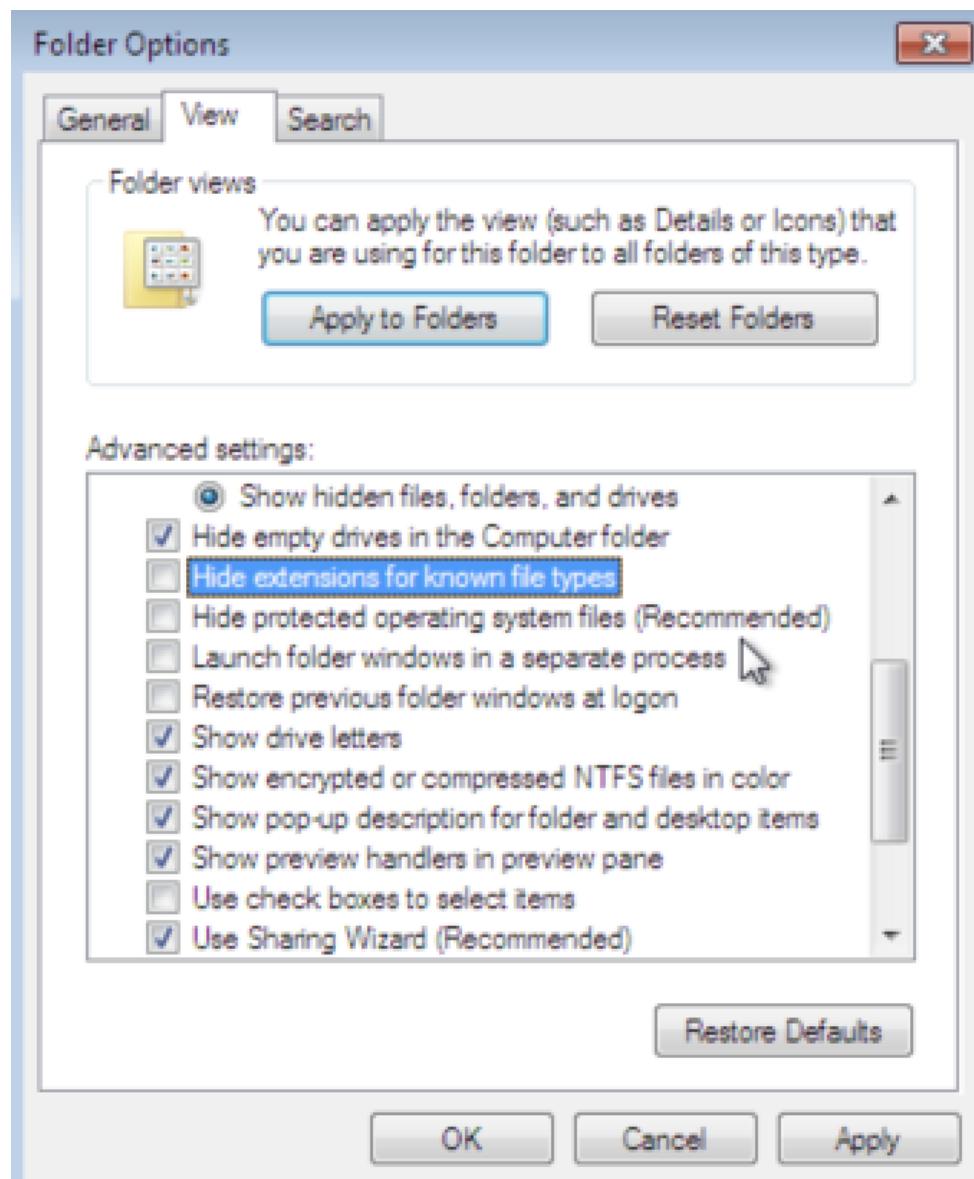
Analiz etmek istediğimiz kötü amaçlı yazılımları engelleyerek veya kaldırarak virüsten koruma yazılımının analizimize müdahale etmesini önlemek için virüsten koruma yazılımını devre dışı bırakmamız gereklidir.

3) Güncellemeleri Devre Dışı Bırak

Kötü amaçlı yazılımlar çeşitli güvenlik açıklarından yararlanıyor olabilir. Dinamik analizimiz sırasında, kötü amaçlı yazılımin bu tür güvenlik açıklarından başarıyla yararlanabilmesi ve çalışmaya devam edebilmesi için sanal işletim sistemimizin güvenlik güncellemelerini almasını engellemeliyiz. Bu nedenle işletim sistemimizin otomatik güncelleme seçenekini devre dışı bırakmalıyız.

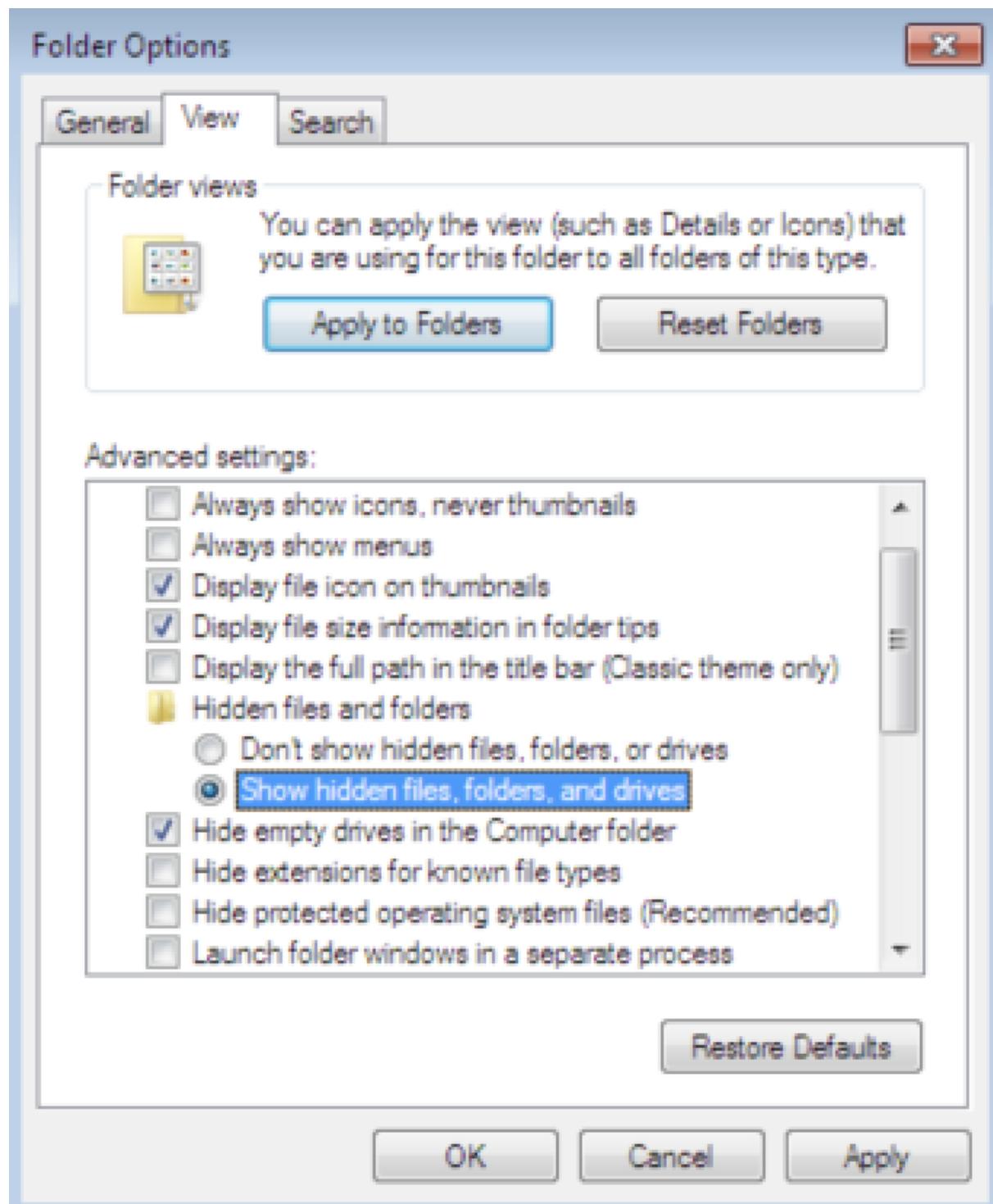
4) Gizli Uzantıları Devre Dışı Bırak

Varsayılan olarak, bilinen dosya uzantıları Windows işletim sisteminde gizlidir. Analiz etmek istediğimiz dosyanın tam adını görebilmemiz için bu özelliği devre dışı bırakmamız gerekiyor.



5) Gizli Dosyaları ve Klasörleri Devre Dışı Bırakın

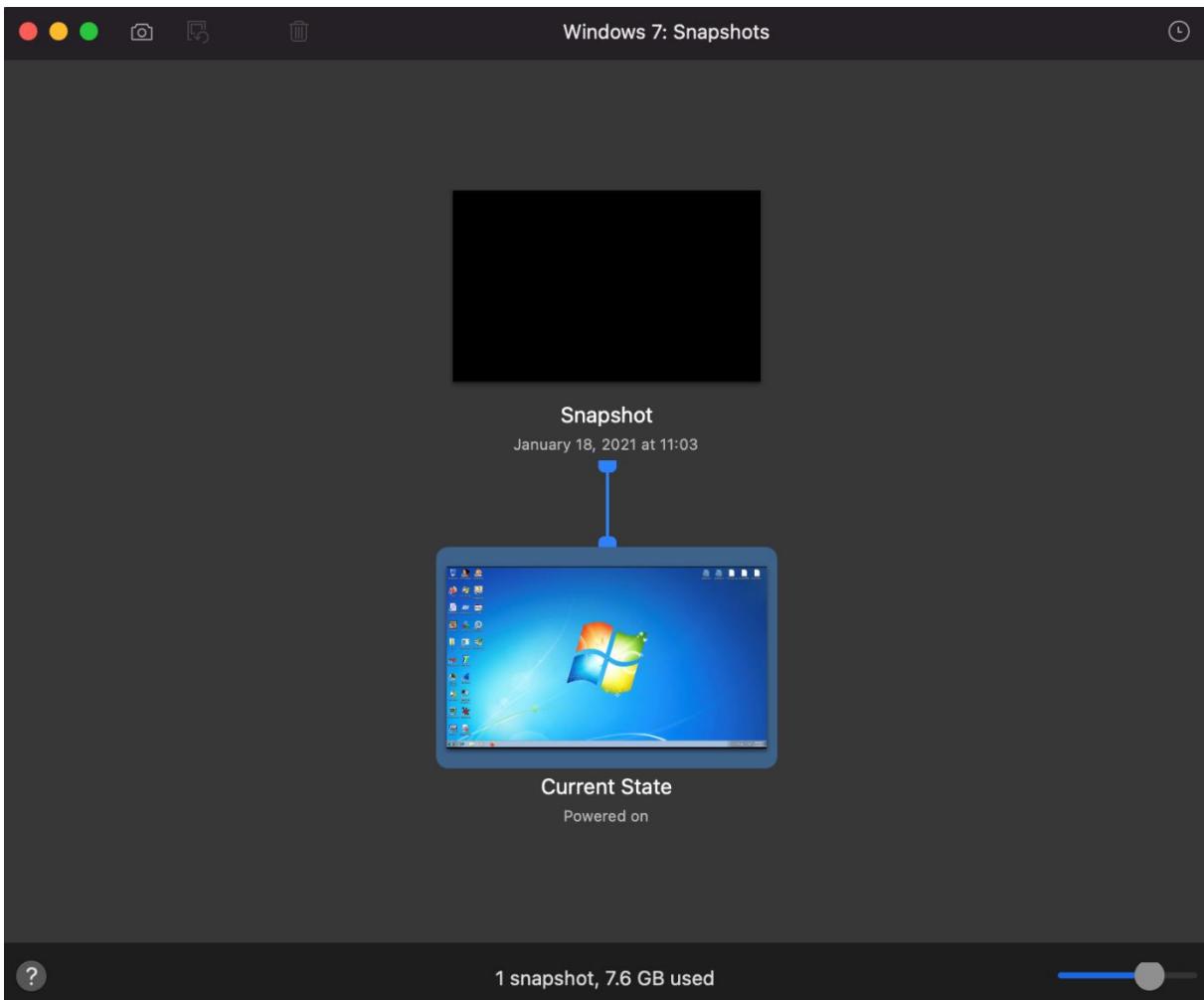
Gizli dosyalar, Windows işletim sisteminde varsayılan olarak görüntülenmez. Kötü amaçlı yazılım, bu özellikten yararlanarak tespit edilmesini zorlaştırır. Dosya sisteminde tam olarak neler olduğunu görmek için bu özelliği devre dışı bırakmamız gerekiyor.



anlık görüntüler

Kötü amaçlı yazılım çalıştırduğumızda, sistemde çeşitli değişiklikler yapar. İşletim sistemini orijinal durumuna döndürmezseniz, yeni bir kötü amaçlı yazılımı analiz ederken çalıştırığınız kötü amaçlı yazılımla karıştırabilirsiniz.

Kötü amaçlı yazılımları her analiz etmek istediğimizde yeni bir sanal işletim sistemi kurmak çok zor olacaktır. Sanallaştırma yazılımının **Snapshot** özelliği işimizi çok kolaylaştırıyor.



Sanallaştırma ortamı üzerinden sanal cihazınızın anlık görüntüsünü aldığınızda, cihazın mevcut durumunu kaydeder. Daha sonra bu anlık görüntüye donecek ve cihazı geri yükleyeceksiniz.

Kötü amaçlı yazılım analizi için gerekli araçları yükledikten sonra, bir anlık görüntü alabilir ve kötü amaçlı yazılımları analiz ettikten sonra bu anlık görüntüye donebilir ve işletim sisteminin orijinal durumuna donebilirsiniz.

Kötü Amaçlı Yazılım Analistinin Araç Kutusu

Kötü amaçlı yazılımları analiz etmek için işimizi kolaylaştıracak hangi araçlara bir göz atalım.

Bir zihin haritası oluşturmak için kötü amaçlı yazılım analizi sırasında kullanabileceğimiz araçları **5** farklı kategoriye ayırdım.

Bizim yazmadığımız ve kötü amaçlı yazılım analizinde kullanılabilecek birçok faydalı araç var. Bu makale, kötü amaçlı yazılım analizinde sıkılıkla karşılaşduğumuz ve kullandığımız araçlardan oluşmaktadır.

1) Parçalayıcılar

Birçok dilde yazılmış bir programın (C, C++ gibi derlenmiş diller) makineler tarafından çalıştırılabilmesi için makinenin anlayabileceği 0 / 1s'ye çevrilmesi gereklidir. Bu işleme derleme denir.

Bir kötü amaçlı yazılımı analiz etmek istediğimizde, bu kötü amaçlı yazılımı 0 / 1s'de analiz etmek neredeyse imkansızdır. Disassembler yazılımı, derlenen yazılımı derleme diline okunabilir ve analiz edilebilir bir formata dönüştürür.

Kullanım kolaylığı, yetenekleri ve birçok dosya formatı desteği nedeniyle, *Hex Rays'in IDA Disassemblers* yazılımı yaygın olarak kullanılmaktadır.

Araç kutunuzda bulunması gereken bir yazılımdır.

2) Hata Ayıklayıcılar

Hata ayıklayıcılar, bir programın çalışmasını adım adım izlememize ve değiştirmemeye ve çalışma zamanında programın kayıtlarını ve yiğinini izlememeye ve kontrol etmemeye izin veren yazılımlardır.

Kullanılan en popüler hata ayıklayıcılarından bazıları aşağıdadır.

1. **IDA Debugger**
2. **Immunity Debugger**
3. **OllyDbg**
4. **Windbg**
5. **x64dbg**

Kötü amaçlı yazılım analizimizde sıkılıkla hata ayıklayıcıları kullanacağız.

3) Dosya Görüntüleyiciler, Düzenleyiciler ve Tanımlama Araçları

PE Dosya Düzenleyicileri, dosyalardaki bilgileri Taşınabilir Yürüttülebilir Dosya Biçiminde okunabilir biçimde görüntüler.

Taşınabilir Yürüttülebilir Dosya Biçimi, bir kötü amaçlı yazılım analisti için önemli olabilecek bilgileri içerir. Örneğin, Image File Header'daki "Machine" bilgisine bakarak, oluşturulan kötü amaçlı yazılımın 32 bit işletim sistemlerini mi yoksa 64 bit işletim sistemlerini mi hedef aldığıni öğrenebilirsiniz.

Aşağıda kullanabileceğiniz bazı araçlar bulunmaktadır.

1. **CFF Gezgini**
 2. **PEGörünüm**
 3. **PEiD**
 4. **BinText (Bunun bir Dosya Düzenleyici olmadığını biliyorum ama size PE Dosyasının içindeki dizeleri gösterebilir)**
 5. **DocFileViewerEX**
 1. **(CFF Explorer**
 2. **PEView**
 3. **PEiD**
 4. **BinText (I know it's not a File Editor but it can show you strings inside PE File)**
 5. **DocFileViewerEX**
-)

4) Ağ Analiz Araçları

Kötü amaçlı yazılım, verileri ele geçirme, komuta kontrol sunucularından komut alma ve ağ içinde yayılma gibi çeşitli etkinlikler için ağ etkinlikleri gerçekleştirir.

Kötü amaçlı yazılımın ağ etkinliklerini izlemek ve analiz etmek için, kötü amaçlı yazılım analistinin araç kutusunda ağ etkinliklerini analiz edebilecek bir araca sahip olması gerekir.

Aşağıda, kullanabileceğiniz bazı ağ analiz araçları bulunmaktadır.

1. **Wireshark**

2. **Fiddler**

5) Diğerleri

Yazımızda bahsettiğimiz araçlar dışında kötü amaçlı yazılım analizinde kullanabileceğiniz ve işinizi kolaylaştıracak birçok araç bulunmaktadır.

Sysinternals içerisinde bulunan **procmon** aracı ile işletim sistemindeki dosya, kayıt defteri ve işlem/iş parçacığı olaylarını görüntüleyebilirsiniz .

Sysinternals içerisinde bulunan **autoruns** aracı ile işletim sisteminde otomatik olarak başlayacak olan işlemleri görebilirsiniz. Kötü amaçlı yazılım, sistemde kalıcılığını sağlamak için genellikle otomatik olarak başlayacak şekilde kendini kaydeder.

Sysinternals araçlarının her biri, kötü amaçlı yazılım analizinde işimizi çok kolaylaştıracak. Bu nedenle, **Sysinternals'ı** araç kutunuza eklemenizi şiddetle tavsiye ederiz. **Sysinternals** içerisindeki araçlar ile bir çok işlemi yapabiliyoruz .

Volatile aracı ile adli tıp analizinizi hafıza üzerinde gerçekleştirebilirsiniz.

İşletim sistemi üzerinde çalışan işlemleri görmek ve izlemek için **Process Hacker**, **Process Explorer** gibi araçları kullanabilirsiniz .

Kötü Amaçlı Yazılımları Analiz Ederken Hangi Yaklaşımı Seçmelisiniz?

Savunma alanında çalışıyorsanız, kötü amaçlı yazılımları analiz etmek işinizin bir parçası haline gelir.

Bu yazımızda zararlı yazılımları hangi yaklaşımlarla analiz edebileceğinizi ve bu yaklaşımların birbirine avantaj/dezavantajlarını ele alacağız.

Kötü amaçlı yazılımları analiz etmek için 2 farklı yaklaşım vardır.

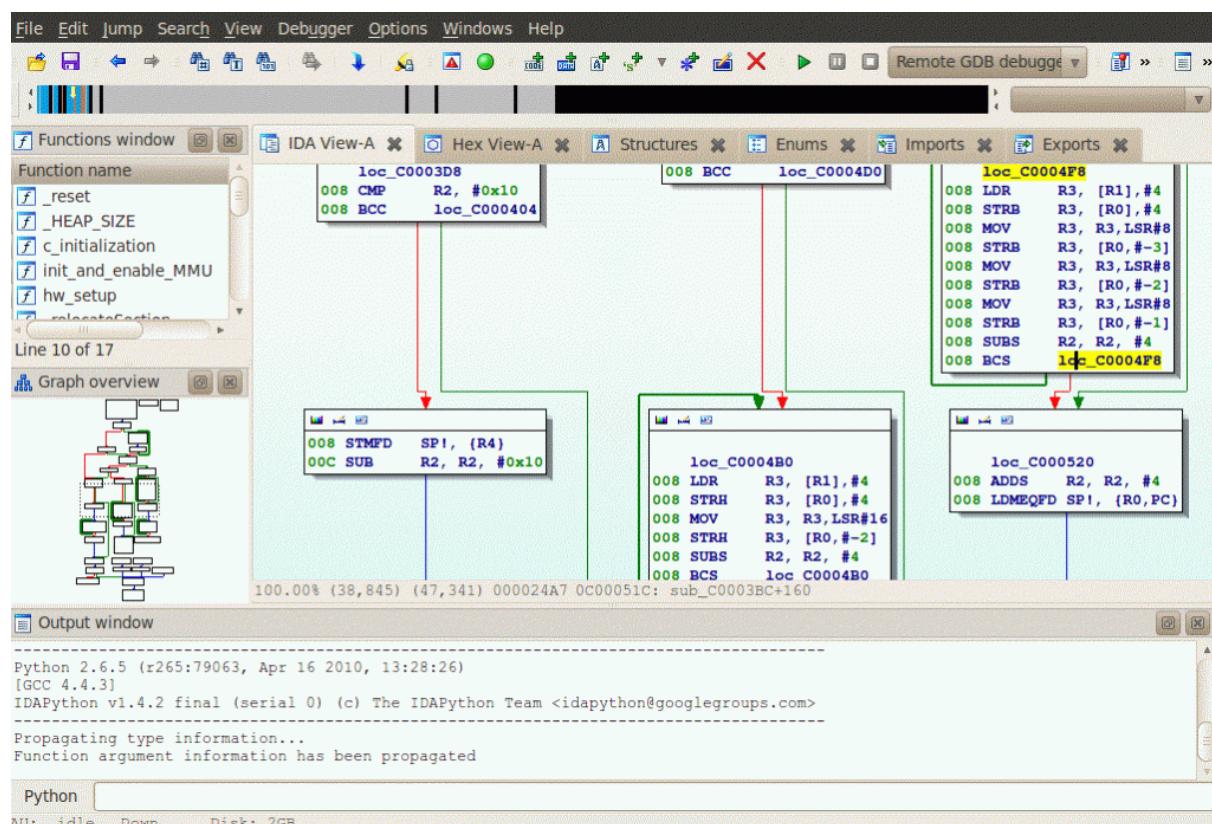
1. Statik Analiz

2. Dinamik Analiz

Statik Analiz Nedir?

Kötü amaçlı yazılımları çalıştırmadan tersine mühendislik yöntemleriyle analiz etme yaklaşımıdır.

Genel olarak, kötü amaçlı yazılımın geri derlenmesi/sökülmesi ile kötü amaçlı yazılımın gerçekleştirileceği her adım analiz edilir, dolayısıyla kötü amaçlı yazılımın davranışı/kapasitesi analiz edilebilir.



https://www.hex-rays.com/products/ida/news/6_0/

Statik analizde kötü amaçlı yazılım çalıştırmadığınız için cihazınıza virüs bulaşmaz. (Ancak, host cihazınızda statik analiz yapmanızı önermiyoruz, analizinizi sanal bir işletim sisteminde yapmanız daha doğru olacaktır.)

Statik analiz sırasında incelenen bilgiler aşağıdaki gibidir.

1. PE (Taşınabilir Yürüttülebilir) Başlıkları
2. İçe aktarılan DLL'ler

3. Dışa aktarılan DLL'ler
4. İkili diziler
5. CPU Talimatları

Dinamik Analiz Nedir?

Kötü amaçlı yazılımların sistem üzerindeki davranışını çalıştırarak inceleyen yaklaşımındır.

Dinamik analizde, sisteme kayıt, dosya, ağ ve işlem olaylarını inceleyebilen uygulamalar yüklenir ve kötü amaçlı yazılımlar çalıştırılarak davranışları incelenir.

Dinamik analiz yaparken aşağıdaki olayları dikkatlice incelemelisiniz.

1. Ağ bağlantıları
2. Dosya Olayları
3. Süreç Olayları
4. Kayıt Olayları

| Process Monitor - Sysinternals: www.sysinternals.com | | | | | | |
|--|-----------------|-------|---------------|---|----------------|----------------------|
| File | Edit | Event | Filter | Tools | Options | Help |
| Time o... | Process Name | PID | Operation | Path | Result | Detail |
| 10:01:51... | lsass.exe | 832 | CreateFile | C:\Windows\System32\Microsoft\Protect... | SUCCESS | Desired Access: G... |
| 10:01:51... | lsass.exe | 832 | CloseFile | C:\Windows\System32\Microsoft\Protect... | SUCCESS | |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryKey | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Query: HandleTag... |
| 10:01:51... | sw2_service.exe | 3732 | RegOpenKey | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Desired Access: R... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Type: REG_DWO... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Type: REG_SZ, Le... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Type: REG_SZ, Le... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Type: REG_SZ, Le... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Type: REG_SZ, Le... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\Software\Microsoft\Cryptography | SUCCESS | Desired Access: R... |
| 10:01:51... | sw2_service.exe | 3732 | RegSetInfoKey | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | KeySetInformation... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Type: REG_SZ, Le... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Type: REG_SZ, Le... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Type: REG_SZ, Le... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Type: REG_SZ, Le... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | Type: REG_SZ, Le... |
| 10:01:51... | sw2_service.exe | 3732 | RegCloseKey | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryKey | HKLML | SUCCESS | Query: HandleTag... |
| 10:01:51... | sw2_service.exe | 3732 | RegOpenKey | HKLML\Software\Microsoft\Cryptography\... | NAME NOT FOUND | Desired Access: R... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryKey | HKLML | SUCCESS | Query: HandleTag... |
| 10:01:51... | sw2_service.exe | 3732 | RegOpenKey | HKLML\Software\Microsoft\Cryptography\... | NAME NOT FOUND | Desired Access: R... |
| 10:01:51... | sw2_service.exe | 3732 | RegCloseKey | HKLML\SOFTWARE\Microsoft\Cryptogra... | SUCCESS | |
| 10:01:51... | sw2_service.exe | 3732 | RegCloseKey | HKLML\SOFTWARE\SecureW2\License | SUCCESS | |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryKey | HKLML | SUCCESS | Query: HandleTag... |
| 10:01:51... | sw2_service.exe | 3732 | RegOpenKey | HKLML\SYSTEM\CurrentControlSet\Servic... | REPARSE | Desired Access: R... |
| 10:01:51... | sw2_service.exe | 3732 | RegOpenKey | HKLML\System\CurrentControlSet\Servic... | SUCCESS | Desired Access: R... |
| 10:01:51... | sw2_service.exe | 3732 | RegQueryValue | HKLML\System\CurrentControlSet\Servic... | NAME NOT FOUND | Length: 144 |
| 10:01:51... | sw2_service.exe | 3732 | RegCloseKey | HKLML\System\CurrentControlSet\Servic... | SUCCESS | |

Showing 460,776 of 956,665 events (48%) Backed by virtual memory

Statik Analiz ve Dinamik Analiz

Kötü amaçlı yazılımları analiz ederken hangi yaklaşımın kullanılacağı mevcut koşullara bağlıdır. Hızlı sonuç almak istediğiniz durumlarda dinamik analizi tercih edebilirsiniz ancak hem statik hem de dinamik analiz yapmadan analizin tamamlandığını söyleyemeyiz.

Ayrıca, tek bir yaklaşımın kullanılmasının kötü amaçlı yazılımları analiz etmek için yeterli olmayabileceğinin unutulmamalıdır. Her iki yaklaşımı birlikte kullanmak sizi zaferde götürecek!

Statik Analiz

Statik analiz uzun zaman alır.

Kötü amaçlı yazılımin kapasitesini öğrenebilirsiniz.

Detaylı analiz sonucu

Dinamik Analiz

Genel olarak dinamik analiz kısa sürer.

Dinamik analiz sonucunda üzerinde çalıştığı sistem üzerindeki aktiviteleri öğrenebilirsiniz.

Analiz sonucu ayrıntılı değil

Sonuç olarak, bir yaklaşımın diğerinden daha iyi olduğunu söyleyemeyiz. Her birinin farklı koşullarda birbirine göre bir avantajı vardır.

Seviye 1-2 SOC analisti olarak çalışıyorsanız, genellikle dinamik analiz yardımcı ile c2 adresini hızlı bir şekilde alarak aksiyon alabilirsiniz.

AnyRun #1 Kullanan Dinamik Analiz Örneği

Kötü amaçlı yazılımları hızlı bir şekilde analiz etmek için korumalı alan hizmetlerinden / ürünlerinden yararlanabilirsiniz.

[AnyRun](#) , kötü amaçlı yazılımları hızlı bir şekilde analiz etmek istediğinizde kullanabileceğiniz etkileşimli bir sanal alan.

AnyRun, ücretli veya ücretsiz kullanım seçeneklerine sahiptir. Ücretsiz olarak yararlanmak istiyorsanız, tüm analizleriniz başkaları tarafından görülebilir, bu nedenle kişisel veri içerebilecek dosyaları AnyRun'a yüklemenizi önermiyoruz. Ayrıca ücretsiz planın kullanım süresi gibi kısıtlamaları vardır.

Kötü amaçlı yazılım analizimiz için AnyRun'u nasıl kullanabiliriz, ne tür çıktılar alabiliriz, gelin birlikte inceleyelim.

Kötü amaçlı yazılımı AbuseCH aracılığıyla analiz etmek için [80b51e872031a2befeb9a0a13e6fc480](#) hash ile indirelim .

İndirdiğimiz kötü amaçlı yazılımları yüklemek için sol menüden " + " (Yeni Görev) butonuna tıklamamız gerekiyor.

The screenshot shows the AnyRun configuration interface with several sections:

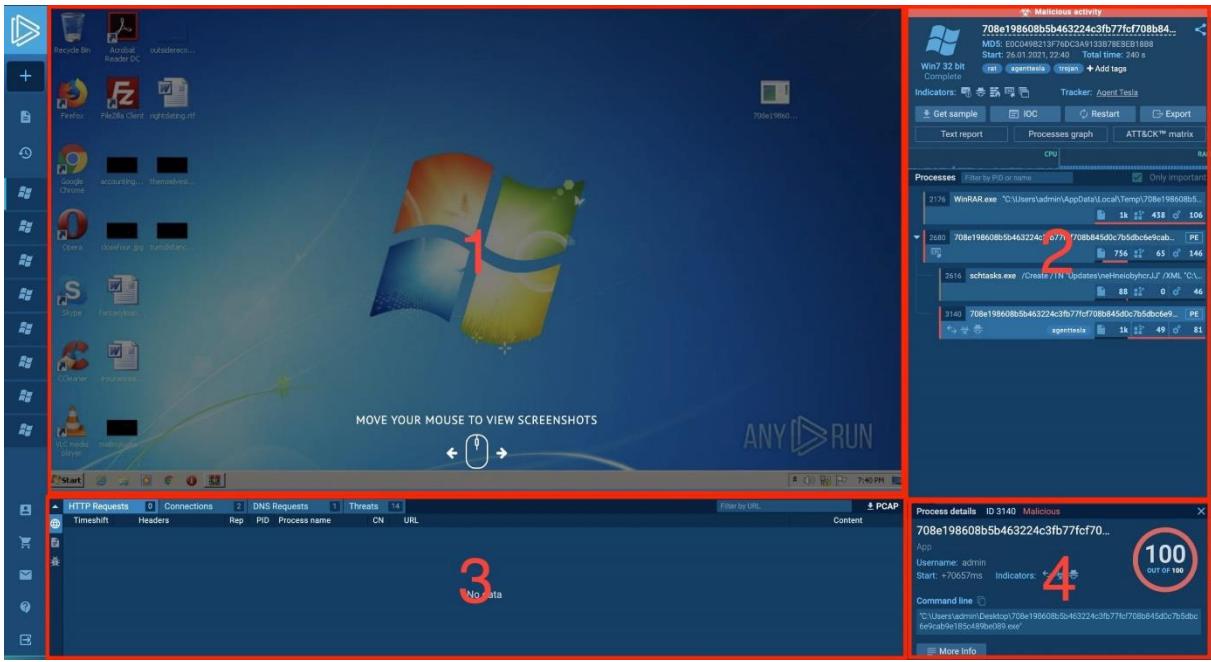
- CHOOSE OPERATING SYSTEM**: Set to Windows 7 (32bit).
- ENVIRONMENT**: Shows installed applications and hot fixes:

| APPLICATIONS | HOT FIXES |
|---|------------------|
| Internet Explorer (KB4534251) | 11.0.9600.195... |
| Microsoft Visual C++ 2013 x86 Additional Run... | 12.0.21005 |
| Microsoft Visual C++ 2013 Redistributable (x8... | 12.0.30501.0 |
| Microsoft Visual C++ 2010 x86 Redistributabl... | 10.0.40219 |
| Google Chrome | 86.0.4240.198 |
| Adobe Acrobat Reader DC | 20.013.20064 |
| Adobe Refresh Manager | 1.8.0 |
| QGA | 2.14.32 |
| Microsoft Visual C++ 2008 Redistributable - x8... | 9.0.30729.6161 |
| Microsoft .NET Framework 4.5.2 | 4.5.51209 |
| Microsoft Office Access Setup Metadata MUI ... | 14.0.6029.1000 |
- OBJECT**: Options for running URLs or files, including "Open in browser" (set to Internet Explorer) and "Download with User Agent" (set to Type User Agent).
- OPTIONS**: Duration (60), Privacy (Public submission), and Network settings:
 - Duration: 60 (or SMART)
 - Privacy: Public submission
 - Network: Connected (Fake Net)
 - Route internet traffic through (optional): Route via TOR, User's VPN (OpenVPN)
 - Network geo: Fastest geo, Choose OpenVPN config
- Buttons at the bottom**: Save as default configuration, Task will be destroyed after 2 weeks, Task will be shared on the Public Submission, Run.

"Dosya seç" butonu yardımı ile açılan ekranda analiz etmek istediğimiz dosyayı upload edelim. Dosya yüklenikten sonra zararlı yazılımı çalıştırmak istediğimiz işletim sistemi ve 32/64 bit işletim sistemi gibi parametreleri belirleyebiliyoruz. Bunları belirledikten sonra açılan ekranın sağ alt kısmında bulunan "**Çalıştır**" butonu yardımıyla sandbox'ımızı açıyoruz .

Makinemiz açıldığında, aktivitelerini görmek için yüklediğimiz kötü amaçlı yazılımı çalıştırırız.

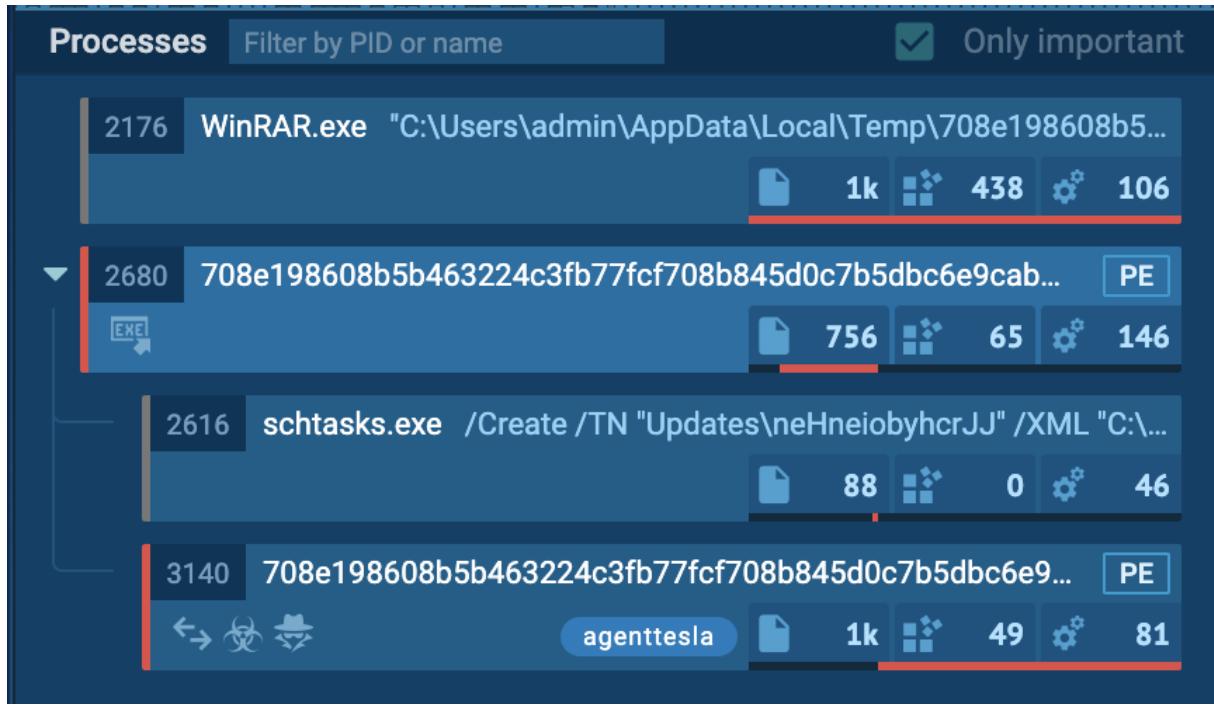
Bazı kötü amaçlı yazılımlar, kötü amaçlı faaliyetlerini gerçekleştirmeden önce belirli bir süre uykuda kalır ve bu da analizi zorlaştırır. Kötü amaçlı yazılımın faaliyetlerini gerçekleştirmesi için zaman tanıyalım, bu süre zarfında AnyRun arayüzüne birlikte inceleyelim.



1. Bu alandan işletim sistemini interaktif olarak kullanabilirsiniz.
2. İşte bu bölümdeki işlemlerin bir listesi. Buradan, çalıştırığınız kötü amaçlı yazılımın hangi alt düzeyde işlediğini kolayca görebilirsiniz.
3. Bu alanda ağ ve dosya olayları vardır.
4. Bu bölüm işlemin ayrıntılarını içerir.

Bu çıktıları inceleyelim.

Öncelikle yukarıdaki görselde "2" ile işaretlenmiş bölümde bulunan zararlı yazılımın işlem olaylarını inceleyelim.



Manuel olarak çalıştırduğumuz kötü amaçlı yazılım, 2 alt süreç oluşturmuş gibi görünüyor. Bunlardan biri, bir zamanlama görevi oluşturarak sistemde kalıcılığı sağlamak için çalıştırılan **schtasks.exe**, diğer ise AnyRun tarafından "**AgentTesla**" malware olarak belirtilen işlemidir.

İşlemler'e tıkladığımızda 4 numaralı panelde bu işlemle ilgili bilgiler görüntüleniyor. Sırasıyla tüm işlemlerin detaylarını inceleyelim.

Kötü amaçlı yazılımı çalıştırmak için arşiv dosyasından çıkardığımızda "WinRAR.exe" adlı işlem oluşturulduğundan, bu işlemi incelemeyeceğiz.

2680 ID ile işleme tıkladığımızda **4** numaralı panelde bu işlemle ilgili bilgiler listeleniyor .

Processes Filter by PID or name Only important

| | PID | Process Name | Path | File | 1k | 438 | 106 |
|------|---|---|------|------|-----|-----|-----|
| 2176 | WinRAR.exe | "C:\Users\admin\AppData\Local\Temp\708e198608b... | | | | | |
| 2680 | 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab... | PE | | | 756 | 65 | 146 |

Process details ID 2680 Malicious

708e198608b5b463224c3fb77fcf708...

App

Username: admin

Start: +16172ms Indicators:

100
OUT OF 100

Command line

"C:\Users\admin\Desktop\708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe"

Danger 2

Uses Task Scheduler to run other applications

Application was dropped or rewritten from another process

Warning 4

Application launched itself

Drops a file with too old compile date

Executable content was dropped or overwritten

Creates files in the user directory

Info 1

Manual execution by user

Bu panelde bulunan " **Daha Fazla Bilgi** " butonu ile işlem hakkında detaylı bilgilerin yer aldığı bir sayfa açılır. Detaylı bilgiye ulaşmak istediğimizde bu bölümü kullanabiliriz.

2680 ID ile işlem bilgileri incelendiğinde kötü amaçlı yazılım:

- Görev Zamanlayıcı'yı kullanır,
- Derleme zamanı çok eski olan bir programı dosya sistemine yazar,
- Kullanıcı dizinine birçok dosya yazar

The screenshot shows a process monitoring interface with the following details:

- Processes** tab selected.
- Filter by PID or name**: sctasks.exe
- Only important** checkbox checked.
- Process details** for ID 2616: No verdict.
- sctasks.exe** details:
 - Manages scheduled tasks.
 - Username: admin
 - A circular rating icon shows **10 OUT OF 100**.
- Command line**:
"C:\Windows\System32\sctasks.exe" /Create /TN "Updates\neHneiobyhcrJJ" /XML "C:\Users\admin\AppData\Local\Temp\tmp5383.tmp"
- More Info** button.
- Danger 1** warning:
Loads the Task Scheduler COM API

2616 nolu işlemi incelediğimizde **Task Scheduler'a** ait **sctasks.exe** olduğunu görüyoruz .

" Komut Satırı " parametrelerini incelediğimizde

" Updates\neHneiobyhcrJJ " adında bir zamanlama görevi oluşturduğunu görüyoruz . Bu zamanlama görevinin konfigürasyonları " tmp5383.tmp " dosyasındadır.

The screenshot shows the VirusTotal analysis interface for the file tmp5383.tmp. At the top, there are three buttons: 'tmp5383.tmp' (with a dropdown arrow), 'Dropped from process' (with a warning icon), and 'Look up on VirusTotal' (with a magnifying glass icon). To the right are two buttons: 'Submit to analysis' (with a circular arrow icon) and 'Download' (with a downward arrow icon). Below these are file metadata: 'Mime: text/xml' and 'Size: 1.58 Kb'. The main area is divided into sections: 'TrID - File Identifier' (showing 100% Generic XML (ASCII)) and 'Hashes' (listing MD5, SHA1, SHA256, and SSDEEP hash values). The 'PREVIEW' tab is selected, displaying the XML configuration of the scheduled task:

```
<StartWhenAvailable>true</StartWhenAvailable>
<RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
<IdleSettings>
    <StopOnIdleEnd>true</StopOnIdleEnd>
    <RestartOnIdle>false</RestartOnIdle>
</IdleSettings>
<AllowStartOnDemand>true</AllowStartOnDemand>
<Enabled>true</Enabled>
<Hidden>false</Hidden>
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<WakeToRun>false</WakeToRun>
<ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
<Priority>7</Priority>
</Settings>
<Actions Context="Author">
    <Exec>
        <Command>C:\Users\admin\AppData\Roaming\neHneiobyhcrJJ.exe</Command>
    </Exec>
</Actions>
</Task>
```

tmp5383.tmp adlı program görev yapılandırma dosyasını incelediğimizde " neHneiobyhcrJJ.exe " adlı programın çalışacağını görüyoruz.

Processes Filter by PID or name Only important

| | |
|------|--|
| 2616 | schtasks.exe /Create /TN "Updates\neHneiobyhcrJJ" /XML "C:\Windows\S... 88 0 46 |
| 3140 | 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e... PE agenttesla 1k 49 81 ↔️ 💀 🕵️ |

Process details ID 3140 Malicious X

708e198608b5b463224c3fb77fcf708...

App

Username: admin

Start: +70657ms Indicators: ↔️ 💀 🕵️

100 OUT OF 100

Command line 🔗

"C:\Users\admin\Desktop\708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe"

☰ More Info

Danger 4

AGENTTESLA was detected

Steals credentials from Web Browsers

Actions looks like stealing of personal data

Application was dropped or rewritten from another process

Warning 3

Reads the cookies of Mozilla Firefox

Reads the cookies of Google Chrome

Creates files in the user directory

ID 3140 ile işlemi incelediğimizde :

- Bu kötü amaçlı yazılım AnyRun tarafından AgentTesla olarak **tanınır**,

- Kimlik bilgilerini çalar,
- Kullanıcı dizininde dosya oluşturma

| Timeshift | Protocol | Rep | PID | Process name | CN | IP | Port | Domain | ASN | Filter by IP | PCAP |
|-----------|----------|------|-----------------------|--------------|-----|----------------|------|-------------------|-----|-------------------|------|
| 162.88 s | TCP | 3140 | 708e198608b5b46322... | | USA | 208.91.199.225 | 587 | smtp.godforeu.com | PDR | ↑ 988 b ↓ 415 b | |
| 165.94 s | TCP | 3140 | 708e198608b5b46322... | | USA | 208.91.199.225 | 587 | smtp.godforeu.com | PDR | ↑ 7.32 Kb ↓ 400 b | |

3 numaralı panelden yapılan ağ bağlantılarını incelediğimizde malware'in **smtp.godforeu.com'a** bağlandığını görüyoruz .

Panelin sağ tarafında bulunan buton yardımı ile gelen/giden datayı inceleyebilirsiniz.

| 208.91.199.225 : 587 ⇄ VM : 51658 | | | | | | | | | | | | | | |
|-----------------------------------|-----------|--|--|--|--|--|--|--|--|--|--|--|--|----------|
| smtp.godforeu.com | | | | | | | | | | | | | | |
| RECV 162.88 s | 00000000: | 32 32 30 20 75 73 32 2E 6F 75 74 62 6F 75 6E 64 00000010: | 2E 6D 61 69 6C 68 6F 73 74 62 6F 78 2E 63 6F 6D 00000020: | 20 45 53 4D 54 50 20 50 6F 73 74 66 69 78 0D 0A | | | | | | | | | | |
| SEND 162.88 s | 00000000: | 45 48 4C 4F 20 55 73 65 72 2D 50 43 0D 0A | | EHLO User-PC.. | | | | | | | | | | |
| RECV 163.89 s | 00000000: | 32 35 30 2D 75 73 32 2E 6F 75 74 62 6F 75 6E 64 00000010: | 2E 6D 61 69 6C 68 6F 73 74 62 6F 78 2E 63 6F 6D 00000020: | 0D 0A 32 35 30 2D 50 49 50 45 4C 49 4E 49 4E 47 00000030: | 0D 0A 32 35 30 2D 53 49 5A 45 20 34 31 36 34 38 00000040: | 31 32 38 0D 0A 32 35 30 2D 56 52 46 59 0D 0A 32 00000050: | 35 30 2D 45 54 52 4E 0D 0A 32 35 30 2D 53 54 41 00000060: | 52 54 54 4C 53 0D 0A 32 35 30 2D 41 55 54 48 20 00000070: | 50 4C 41 49 4E 20 4C 4F 47 49 4E 0D 0A 32 35 30 00000080: | 2D 41 55 54 48 3D 50 4C 41 49 4E 20 4C 4F 47 49 00000090: | 4E 0D 0A 32 35 30 2D 45 4E 48 41 4E 43 45 44 53 000000A0: | 54 41 54 55 53 43 4F 44 45 53 0D 0A 32 35 30 2D 000000B0: | 38 42 49 54 4D 49 4D 45 0D 0A 32 35 30 20 44 53 000000C0: | 4E 0D 0A |
| SEND 163.89 s | 00000000: | 41 55 54 48 20 6C 6F 67 69 6E 20 62 47 39 6E 63 00000010: | 30 42 6E 62 32 52 6D 62 33 4A 6C 64 53 35 6A 62 00000020: | 32 30 3D 0D 0A | | | | | | | | | | |
| RECV 163.89 | 00000000: | 33 33 34 20 55 47 46 7A 63 33 64 76 63 6D 51 36 | 334 UGFzc3dvcnQ6 | .. | | | | | | | | | | |
| | 00000010: | 0D 0A | | | | | | | | | | | | |

Kötü amaçlı yazılımın ağ aktiviteleri incelendiğinde, kötü amaçlı yazılımın SMTP protokolü ile verileri sızdırduğunu görüyoruz.

Kötü Amaçlı Yazılımları Daha Hızlı Analiz Edecek 29 Adres

Kötü amaçlı yazılımları analiz etmek için sürekli zaman harcıyoruz. **Mavi ekip** üyelerinin zamanı daha etkin kullanmaları için faydalı olabilecek 29 adresi listeledik :

- [Anlyz](#)
- [Any.run](#)
- [Comodo Valkyrie](#)
- [Cuckoo](#)
- [Hybrid Analysis](#)
- [Intezer Analyze](#)
- [SecondWrite Malware Deepview](#)
- [Jevereg](#)
- [IObit Cloud](#)
- [BinaryGuard](#)
- [BitBlaze](#)
- [SandDroid](#)
- [Joe Sandbox](#)
- [AMAAaaS](#)
- [IRIS-H](#)
- [Gatewatcher Intelligence](#)
- [Hatching Triage](#)
- [InQuest Labs](#)
- [Manalyzer](#)
- [SandBlast Analysis](#)
- [SNDBOX](#)
- [firmware](#)
- [opswat](#)

- [virusade](#)
- [virustotal](#)
- [malware config](#)
- [malware hunter team](#)
- [virscan](#)
- [jotti](#)