Chapter 3 Labs

* Temel dinamik analiz tekniğini kullanmak için bir kaç adet malware senaryosu inceleyeceğiz.

Lab 3-1

* Temel dinamik analiz tekniğini ve araçlarını kullanarak Lab03-01.exe programının analiz edilmesi isteniyor.

Sorular:

1. Zararlı yazılımın import ve string'leri nelerdir?

   Aslında bir yazılımın import ve string'lerine bakıyor olmak Temel Statik Analiz'dir. Şüpheli yazılımın import ve string lerine bakarak Temel Dinamik Analiz için bir ipucu yakalamaya çalışacağız.

2. Zararlı yazılımın host-based indikatörleri nelerdir?

   Yani şüpheli yazılımı çalıştırın ve bilgisayarda neler yaptığını inceleyin. Yardımcı araçlar kullanarak bu programın (dosya yazma, dosya yaratma, dosya silme, register kayıtlarını değiştirme vb.) neler yaptığının anlaşılması gerekir.

3. Zararlı yazılımın network ile ilgili indikatörleri var mı, varsa nelerdir?

   Yani zararlı yazılım ağ üzerinde paket alış verişi yapıyor mu, yapıyor ise bu durum kritik mi, tehlikeli mi?

* Cevap 3-1-1

Zararlı yazılım hakkında temel bazı bilgiler edinmek için önce temel statik analiz yapılıyor. Yazılım PEview programı ile açılıyor ve import'larına bakılıyor, Yazılımın fazla import'u yok, sadece kernel32.dll import edilmiş. Dolayısı ile yazılımın paketlenmiş olduğu anlaşılıyor. Çünkü bir yazılımın daha fazla import içermesi beklenir.

Sadece import'larına bakılarak şüpheli yazılım hakkında bilgi edinilemedi. Programın paketlenmiş olduğu dolayısı ile import ile ilgili bilgilerin Runtime'da görülebileceği kanısına varıldı.

* Daha sonra programın string bilgilerine bakılıyor. Bunun için aracı bir program veya terminal komutları (string, more) kullanılabilir. Veya VirusTotal gibi internet tabanlı bir platform kullanılabilir.

Programın String ifadelerini çok net görebiliyoruz. Demek ki biraz önce zannettiğimiz gibi program paketlenmemiş veya gizlenmemiş. Halbuki import'larına bakarken çok az sayıda import olduğu için programın paketlenmiş olabileceğini düşünmüştük.

Hatırlarsanız zararlı yazılımların çok az DLL import ettiklerinin altını çizmiştik. Bu durum onların ayırt edici özelliklerinden bir tanesiydi. Bu saatten sonra yazılım hakkındaki şüphelerimiz arttı.

Yazılımın String ifadeleri şekilde açıkça görülebilmektedir. Bu String'ler içerisinde ilginç olanlar var.

→ Register lokasyonları → Register ile ilgili işlemler yapacak ama ne?
→ Domain name → Bir siteye bağlanarak veri alış verişi yapacak ama ne?
(5) → WinVMX32 → ???
→ VideoDriver → Masum bir yazılım neden videodriver isimli bir String kullanır?
→ vmx32to64.exe → Bu exe'yi çalıştırmayı mi deneyecek?

Buradaki soruların cevabını temel dinamik analiz ile verebiliriz.

* Cevap 3-1-2

Temel dinamik analize başlamadan önce bazı ayarların yapılması gerekiyor:

1) Güvenilir ortam (sanal veya fiziksel)
2) Process Explorer programı çalıştırılır.
3) Procmon programı çalıştırılarak önceki event'lar silinir, filtre varsayılan ayarlara getirilir.
(6)
4) Virtual Network için gerekli konfigürasyonlar yapılır.
(7)
5) ApateDNS çalıştırılır. (domain var programda)
6) Netcat çalıştırılıp TCP port 80 (http) ve 443 (https) dinlenecek şekilde ayarlanır.
7) Wireshark çalıştırılır (paket dinlemek gerekebilir).

Ayarlamalar yapıldıktan sonra şüpheli yazılımı çalıştırıyoruz.

Process Explorer programında Lab03-01.exe'yi seçerek

View > LowerPane View > Handles penceresini açıyoruz. Burada programın kullandığı kaynaklar gösterilir.

Bir program; bir dosyayı, bir ileti sırasını, ağ bağlantısı ve kayıt defteri gibi bazı sistem kaynaklarını kullanıyor ise bu Handle penceresinde görülür.

Handle penceresine bakıldığında programın WinVMX32 isimli bir mutex oluşturduğu görülür.

Mutex; Bir program birden fazla iş parçacığı veya işlem arasında senkronizasyon sağlamak için mutex oluşturabilir. Mutex "mutually exclusion" kelimelerinin kısaltılmasıdır ve kritik bir bölgeye tek bir iş parçacığının veya process'in aynı anda erişmesini sağlayan bir senkronizasyon mekanizmasıdır.

7

Mutex'ler genellikle paylaşılan kaynaklara erişimi kontrol etmek için kullanılırlar. Örneğin bir dosyaya yazma işlemi gerçekleştiren iki farklı iş parçacığı varsa bu iş parçacıklarının aynı anda dosyaya yazmaya çalışmamasını sağlamak için mutex kullanılabilir. Bir iş parçacığı dosyaya yazma işlemini başlatırken mutex'i kitler ve işlemini tamamladığında mutex'i serbest bırakır. Diğer iş parçacıkları dosyaya erişmek istediklerinde mutex kilidini almak için beklerler ve bu şekilde kritik kaynağa sıra ile erişilir.

* Process Explorer programının limitleri buraya kadar. Şu anki vaka üzerinde yapması gerekeni yaptı, Arka planda procmon programı çalışıyordu ve makinede çalışan programların gerçekleştirdiği her event'i kaydediyor.

Bilgisayar sisteminde saniyeler içerisinde on binlerce event (olay) gerçekleşir. Dolayısı ile hepsini incelememiz olanaksız. Bu sebeple amacımıza yönelik filtre kullanmamız gerekir. Process Explorer programında elde edilen verileri kullanarak spesifik filtreler yazacağız.

(8) Buradaki örnekte 3 adet filtre yazılmış:

1) Process Name is Lab03-01.exe
2) Operation is RegSetValue
3) Operation is WriteFile

Yani Lab03-01.exe isimli programın "RegSetValue" ve "WriteFile" event'larını incelemek istiyoruz.

* Yazılan birleşik filtreyi uyguladığımızda procmon programındaki kayıtlar 10'a düşüyor. Bu kayıtlardan bir tanesi dosya yazma diğer 9 tanesi register set etme olayı.

(9) Register olaylarının 8 tanesi de aslında ciddi bir olay değil. Zararlı yazılımı yazan kişi yaptığı kritik işlemi saklamak için bunları fazladan oluşturmuş yani yazılımın incelenmesini güçleştirmek için gürültü eklemiş.

Gürültü amacı ile eklenmiş kayıtlar rastgele sayı üretecini güncelliyor. Ve bu önemsiz bir işlem.

Listede görünen 10 event içerisinden sadece 2 tanesi önemli, şekildeki 1 ve 2 numaralı aktiviteler. Bir tanesi bir dosyaya yazma event'i, diğeri ise bir Register değeri set etme işlemi.

* Kritik bu iki kayıttan ilki bir WriteFile event'i. Event'a tıklayarak ayrıntılı bilgi ediniyoruz.

C:\WINDOWS\System32\ klasörünün içerisine vmx32to64.exe isimli bir dosya kopyalanmış ve bu dosyanın boyutu incelenen
(10) şüpheli yazılım ile aynı yani 7,168 byte.

Ayrıca bu dosyanın MD5 hash değeri de Lab03-01.exe dosyası ile aynı. Yani program kendini System32 klasörünün içine kopyalamış ve ismini de vmx32to64.exe yapmış, sanki bir driver ismi gibi.

* Daha sonra ikinci kritik kayıt olan register event'ına bakalım. Kayıda çift tıklayıp zararlı yazılımın register'a ne yazdığına yani ayrıntıya kalkıyoruz.

(11) Register'a yeni bir kayıt eklenmiş olduğunu görüyoruz:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
lokasyonuna yeni bir register anahtarı eklenmiş ve anahtarın ismi VideoDriver.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run register adresi Windows başlatıldığında otomatik olarak başlatılacak programların ve hizmetlerin listelendiği yerdir. Kayıt defterinin bu bölümündeki girdiler Windows başlangıcında çalışacak programların yollarını içerir.

Zaten zararlı yazılımda Windows açıldığında başlamak için kendini C:\Windows\System32 klasörünün altına vmx32to64.exe ismi ile kopyalıyor.

* Cevap 3-1-3

3. soruda network aktiviteleri var mı, varsa nelerdir? Bunlara bakmamız isteniyor.

İlk başta zararlı yazılım herhangi bir DNS sorgusu gerçekleştirmiş mi diye bakıyoruz. ApateDNS programını açtığımızda zararlı yazılımın www.practicalmalwareanalysis.com isimli domain'i sorguladığını görüyoruz, zaten ilk string araştırmasında da bunu anlamıştık.

Başka bir DNS sorgusu yapılacak mı diye bir süre beklenebilir.

Daha sonra Netcat programından belli başlı servislerin kullanıldığı port'ları dinleyebiliriz ki en başta Netcat TCP 80 ve 443 port'larını dinleyecek şekilde ayarlanmıştı. TCP 80 Http, 443 ise Https protokolü kullanır.

* Mesela bu örnekteki şüpheli yazılım TCP 443 portundan rastgele gibi görünen garip mesajlar göndermiş. Program bir kaç defa çalıştırılmış ve her seferinde farklı bazı rastgele veriler bu port'tan gönderilmiş.

Bu mesaj paketinin içeriğine bakılması gerekiyor. Ne mesaj, şifrelenmiş veri mi, nedir?

Bir paket yakalayıcı olan Wireshark ile paket yakalanıyor ve inceleniyor. Bu paketin 256 byte büyüklüğündeki beacon paketleri olduğu anlaşılıyor.

13 Beacon Protokolü: Genellikle kötü amaçlı yazılımlar tarafından kullanılan bir iletişim protokolüdür. Bu protokol, enfekte edilmiş bir cihazın genellikle kötü amaçlı bir yazılım tarafından kontrol edilen bir komuta ve kontrol sunucusuna düzenli olarak "beacon" yani sinyal göndermesine dayanır. Bu sinyaller enfekte cihazın hala aktif olduğunu belirtir.

Beacon protokolü, kötü niyetli bir saldırganın enfekte ettiği cihazları kontrol etmek ve yönetmek için kullanılan bir araç olarak işlev görür. Bu protokol enfekte edilmiş cihazların arka planda sessizce çalışmasına ve kontrol sunucusundan gelen talimatları uygulamasına izin verir.

Lab 3-2

* Lab03-02.dll dosyası çalıştırılarak analiz edilmesi isteniyor.

Sorular

1. Bu kötü amaçlı yazılımın kendi kendine yüklenmesini nasıl sağlayabiliriz?
2. Kötü amaçlı yazılımın kurulumundan sonra çalışmasını nasıl sağlayabiliriz?
3. Zararlı yazılım çalıştırıldığında arkada işleyen process'i nasıl bulabiliriz?
4. Procmon'dan kullanışlı bilgiyi almak için hangi filtreleri kullanmalıyız?
5. Zararlı yazılımın makine tabanlı indikatörleri nelerdir?
6. Zararlı yazılım için kullanışlı bazı network indikatörleri var mıdır?

* Cevap 3-2-1

Öncelikle yine zararlı yazılım hakkında hızlı ve temel bir veriye sahip olabilmek için temel statik analiz ile başlıyoruz ve malware'ın PE dosya yapısına ve string'lerine bakıyoruz. DLL dosyalarının genellikle export yapmasını bekleriz. O yüzden şekilde de görüldüğü üzere PEview'dan malware'ın export'larına bakıyoruz.

Şüpheli yazılımın 5 adet export'u var ve bunlardan bir tanesi "install" diğeri de "ServiceMain". Bu iki export'tan şunu anlıyoruz: Yazılımın düzgün çalışabilmesi için bir servis olarak yüklenmesi gerekir.

* Daha sonra şüpheli yazılımın string ifadelerine bakıyoruz. Import edilen birçok fonksiyon var tehlikeli olanlar şekilde koyu renk ile gösterilmiş.

Import edilen bu kritik fonksiyonların arasında şüpheli yazılımın
(17) servisleri manipule etmesine olanak tanıyan CreateService, register'ı manipule etmesini sağlayan RegSetValueEx gibi fonksiyonlar var. Ve HttpSendRequest gibi network ile ilgili bazı fonksiyonlar import etmiş. Bu da bize Http porotokolünü kullanacağını gösteriyor.

* Şüpheli yazılımın string'lerine bakmaya devam ediyoruz. Listenin devamında yine ilginç bazı başka string'ler var.

→ registery lokasyonları
→ domain ismi
(18) → serve.html
→ tek başına garip bir string ifade IPRIP

Şimdi temel dinamik analiz tekniği de bu string'lerin nasıl kullanılacağını, kullanıldığını gösterecek.

* Cevap 3-2-2

Temel statik analiz tekniğinden elde ettiğimiz bulguya göre; bu şüpheli yazılımın export ettiği installA isimli fonksiyonu kullanarak servis olarak kurulmasına ihtiyaç var.

Fonksiyonu rundll32.exe komutu ile çalıştıracağız. Ancak öncelikle Regshot kullanarak registry'nin bir imajını alıyoruz ve Process Explorer programını başlatıyoruz.

(19) Şekilde de görüldüğü gibi fonksiyonu komut satırından;

C:\>rundll32.exe Lab03-02.dll, installA

olarak çalıştırıyoruz.

Daha sonra Regshot programını kullanarak sistemin registry'sinin ikinci imajını alıyoruz. Amacımız programın kendini registry'e yükleyip yüklemediğini anlamak.

* Alınan iki register kaydını karşılaştırıyoruz ve registry'e bazı
(20) kayıtların eklendiğini görüyoruz.

* ① numaradan şu anlaşılıyor: Şüpheli yazılım kendini registry'e IPRIP isimli bir servis olarak kaydetmiş.

② Şüpheli yazılım bir DLL yani başlayabilmesi için başka bir
(21) çalıştırılabilir dosyaya bağımlı. ImagePath dizini svchost.exe olarak set edilmiş. Bu şüpheli yazılımın svchost.exe process'i içerisinden başlatılacağını gösteriyor.

③ ve ④ 'te ise DisplayName ve Description anahtarları ile kötü amaçlı yazılımı tanımlamak için bir kimlik oluşturulmuş. Yani servis olarak görünecek bu yazılımın ne servisi verdiği ile ile ilgili bir tanımlama yapılmış.

* Şüpheli yazılım servis olarak kuruldu ve artık çalıştırıp ne yaptığını inceleyeceğiz. Ama önce procmon'u çalıştırıp event'ları siliyoruz ve filtreyi sıfırlıyoruz yani varsayılan yapıyoruz. Process Explorer'ı başlatıyoruz. ApateDNS ve Netcat kullanarak sanal bir ağ oluşturuyoruz ve Netcat programını TCP 80 portu'nu dinleyecek şekilde ayarlıyoruz.

(22) Bu zararlı yazılım IPRIP servisi olarak kurulduğu için Windows un komut satırından bu şekilde başlatıyoruz.

```
C:\> net start IPRIP
```

Görünürdeki ismi yani DisplayName INA+'tı. Ve bu isimle process olarak başladı. Registry'de bu şekilde tanımlanmıştı.

* Cevap 3-2-3

Process Explorer programında bir sürü svchost.exe olabilir.
Find > Find Handle or DLL kısmından Lab03-02.dll yazıyoruz ve
(23) ilgili svchost.exe'yi buluyoruz. Şekle göre PID'si 1024 olan
(24) bizim ilgilendiğimiz svchost.exe process'i.

Process Explorer'da View > Lower Pane View > DLLs seçiyoruz ve svchost.exe'nin import ettiği DLL'lerine bakıyoruz. Burada svchost.exe'nin Lab03-02.dll'i import ettiğini ve DisplayName'ni görüyoruz. INA+

✳ Cevap 3-2-3 ve Cevap 3-2-4

Procmon'da, Process Explorer'da bulduğumuz PID'e göre filtrelersek istenilen sonuçlara daha hızlı ulaşabiliriz.

Cevap 3-2-6

Daha sonra network araçları ile yazılımın network'te neler yaptığına bakacağız.

İlk önce ApateDNS'i kontrol ediyoruz ve zararlı yazılımın bir DNS isteği yaptığını görüyoruz. IP'sini istediği Domain ismi bizim daha öncesinde string ifadelerinde de gördüğümüz practicalmalwareanalysis.com

(25)

Zararlı yazılımın network trafiğine başlaması 60 saniye sonra oluyor. Bu da demek oluyor ki yazılım Sleep(60000) ile 60 saniye uyutulmuş ve eğer network'te bir sorun var ise tekrar bağlantı isteği için 10 dakika bekliyor.

✳ Network analizlerine Netcat sonuçlarına bakarak devam ediyoruz. Netcat ile TCP 80 port'unu dinliyorduk. Zaten şekilde de görüldüğü üzere bu port üzerinden bağlantı isteği gelmiş. Zararlı yazılım 80 portundan HTTP 1.1 versiyonu ile serve.html dosyasını istiyor.

Kullandığı makine MalwareAnalysis2 Windows XP 6.11 olarak görülüyor. Bu analizin yapıldığı makine.

Lab 3-3

* Lab03-03.exe dosyasını güvenli bir ortamda çalıştırarak temel dinamik araçları ile gözlemleyiniz.

Sorular

1. Zararlı yazılımı Process Explorer ile gözlemleyince neler dikkatinizi çekti?

(27) 2. Yaşayan bellek modifikasyonu (process replecament) tespit edildi mi?

3. Zararlı yazılımın makine-tabanlı indikatörleri nelerdir?

4. Bu programın amacı nedir?

* ## Cevap 3-3-1

Process Explorer ve procmon'u çalıştırıyoruz. Eğer procmon programının capture (yakala) modu açık ise daha açar açmaz bir sürü event yakalamaya başlayacak. En doğru kullanımı ana-

(28) lize hazır olana kadar capture modunu kapalı tutmak. Procmon'da Filter > Filter menüsüne giderek filtreleri reset'leyelim ve sadece default filtrelerin olduğundan emin olalım.

* Lab03-03.exe'yi çalıştırdığımızda Process Explorer'da bu isimde bir process olmadığını görüyoruz. Program svchost.e ismi ile

(29) çalışmakta. Burada şu sebeplerden ötürü şüphelenmemiz gerekir:

1) Neden farklı bir isim ile çalışıyor?
2) Neden bir Windows servisinin ismi ile çalışıyor?
3) Ayrıca bu svchost.exe öksüz bir process, svchost.exe Windows taki servicess.exe tarafından başlatılan ve ebeveyni olan bir process'tir. Genellikle direk başlamaz, burada genel kullanıma aykırı bir durum var.

* Cevap 3-3-2

Daha derin bir araştırma yapmak için bu öksüz svchost.exe process ine sağ-tık yapıp özelliklerini (properties) açıyoruz.

(30) Properties penceresinden strings sekmesine geçip programın ve
(31) process'in "Image" ve "Memory" radio-button'larını kullanarak ayrı ayrı diskteki ve bellekteki string ifadelerine bakıyoruz. Şekilde de görüldüğü üzere şu an Ram'de çalışan process'in farklı string'leri var. ENTER, SHIFT, TAB, BACKSPACE vb.

* Cevap 3-3-3 ve Cevap 3-3-4

Process'in string'lerinin arasında bir log dosyasının
(32) (practicalmalwareanalysis.log) olması ve ENTER, SHIFT, TAB gibi bazı klavye tuşlarının isimlerinin olması bu process'in bir key-logger olabileceğini düşündürüyor.

Bu varsayımı test etmek için bir Netepad açıp kısa bir mesaj yazıyoruz. Process Explorer'dan öksüz olan svchost.exe'nin PID'ini alıp procmon programına geçiyoruz. Procmon'da PID filtresi, CreateFile ve WriteFile filtrelerini yazıyoruz

* Bu zararlı yazılımın svchost.exe üzerinden process replacement yaparak klavye vuruşlarını yakalayarak bir log dosyasına kaydettiğini yani keylogger'lik yaptığını anlıyoruz.

Lab 3-4

* Lab03-04.exe'yi çalıştırıp temel dinamik analiz tekniği ile inceleyiniz. Program temel dinamik analiz tekniği ile incelenemediği için bu program daha ileriki konularda (chapter 9) incelenmiştir.

Sorular

1. Program çalıştırıldığında ne oldu?
2. Dinamik analiz neden yetersiz kaldı?
3. Bu programı çalıştırmanın başka bir yolu var mı?

* ### Cevap 3-4-1 ve Cevap 3-4-2

Temel statik analiz ile PE dosya yapısını ve string'leri inceleyerek analize başlıyoruz. Bu string ifadelerden anlaşıldığı kadarı ile bu şüpheli yazılım network fonksiyonelliği, servis manipulasyonu ile ilgili fonksiyonlar ve registry manipulasyonu ile ilgili fonksiyonlar içeriyor.

* String'lerin içerisinde şüpheli olarak;
  → Registry lokasyonları var,
  → DOWNLOAD ve UPLOAD ifadeleri var.
  → HTTP/1.0 var. Bu HTTP protokolü ile bir backdoor yapabileceğini gösteriyor.
  → -cc, -re ve -in gibi komut satırı parametreleri var, Örneğin buradaki -in parametresi ile bir programı install ediyor olabilir.

Şimdi ise temel dinamik analiz teknik ve araçlarını kullanarak bu şüphelerimizin doğru olup olmadığına bakmamız gerekir.

Şüpheli programı çalıştırmadan önce analiz araçlarımız Process
(37) Explorer ve Procmon'u çalıştırıp Sanal Ağı kuruyoruz.

Şüpheli programı çalıştırdığımızda process hızlı bir şekilde başlıyor, işini yapıyor ve sonlanıyor. Ayrıca disk'teki programı da siliyor. Dolayısı ile hiçbir şey görülemiyor ve tabiki analiz sağlıklı bir şekilde yapılamıyor.

procmon programından Lab03-04.exe darak filtrelediğimizde ise ilginç bir WriteFile veya RegSetValue işlemi görünmüyor. Ancak başka bir process ismi ile kritik işlemler gerçekleştirmiş olabilir.

* Fakat Process Create işlemi yapılmış ve çift tıklama yaparak
(38) ayrıntıya bakıyoruz. şekilde de görüldüğü üzere process komut satırını kullanarak disktekl programı silmiş.

* Program komut satırından -in, -re ve -cc komutları ile çalış-
(39) tırılsa bile kendini siliyor. Dolayısı ile ayrıntılı bir analiz yapılamıyor.