**SANDBOX**

Günümüzde kum havuzu (sandbox) teknolojileri basit düzeyden gelişmiş düzeye dek ürünler içerisinde ve ürünlerden bağımsız olarak ürünleşmiş şekilde kullanılır durumdadır. Bazı antivirüs programlarının içerisinde de kum havuzu (sandbox) teknolojilerinden faydalanılmaktadır, ancak bu ürünlerde gerçek anlamda bir analiz yapılmamakta, imza tabanına ek bir güvenlik ile hızlı ve pratik bir dinamik analiz sunulmakta, böylelikle daha başarılı bir koruma yapılmaktadır.

Kum havuzu teknolojileri bazı markalarca ürünleştirilirken donanım ile bütünleşik şekilde tutulmuş, kullanıcının bulunduğu alanda yer alan kaynakların incelenmesi sağlanmıştır. Ancak bu tutum zamanla mobilitesi artan kullanıcılar için yetersiz kalmaya başlamış, bulunulan ağ artık dağınık bir ağ olduğundan çözüm yetersiz kalmaya başlamıştır.

Mobilitenin artmasıyla birlikte kullanıcıların (istemcilerin) kendi cihazları üzerinde, uç noktada güvenliğin sağlanması ihtiyacı doğmuştur. Ancak şu an tüm işlemlerin kullanıcı cihazı üzerinde gerçekleştirilmesi için yeterli işlemci gücü kaynağı veya kullanıcının tercihi bulunmamaktadır.

Zira işlem gücünü direkt olarak etkilemesinden ötürü kullanıcılar genellikle cihazlarını yavaşlatan mekanizmaları devredışı bırakma eğilimindedirler.

Merkeze erişim sağlanan çözümler yer ve cihaz bağımsız gerçekleştirilebildiğinden, son yıllarda popüler ve ekonomik çözümler olarak dikkat çekmektedir. Merkez üzerinde daha kuvvetli işlemcilere işlem güçlerinin aktarılması, işlemci tasarrufu, enerji (pil) tasarrufu ve zaman tasarrufu sağlamakta ayrıca merkez üzerinde birleşen verilerden (big data olarak da adlandırılmaktadır) tüm kaynaklar eş zamanlı olarak faydalanabildiğinden yüksek örnek toplama şansı dolayısıyla başarı artmakta ve kullanıcılara ek fayda sağlanmaktadır.

Proje ile oluşturulacak yapı antivirüs teknolojilerinde kullanıcı üzerindeki işlemci yükünü almak, tam bir analiz gerçekleştirerek sandbox atlatan yazılımları da tespit edebilmek konularında gelişme sağlayacaktır. Ayrıca e-posta eklentileri üzerinde de aktif olarak çalışması özellikle ulusal seviyede önlem alınabilmesi açısından büyük fayda sağlayacaktır.

**Referanslar**

* Alexandros Kapravelos Yan Shoshitaishvili - Marco Cova - Christopher Kruegel - Giovanni Vigna Revolver: An Automated Approach to the Detection of Evasive Web-based Malware
* 01.01.2013 -
* Web tabanlı zararlı yazılımların fark edilmeyi engelleyen yöntemlerine karşı uygulanabilecek sınıflandırma yöntemi
* Breaking the Sandbox 01.01.2015 - Sudeep Singh Sandbox'tan kaçma metotları, tespit ve atlatmalara yönelik yeni uygulamalar incelenecek ve bu metotlara önlemler alınacak
* Detecting Malware and Sandbox Evasion Techniques 01.01.2016 Dilshan Keragala Sandbox'tan kaçma-saklanma metotları üzerine alınacak önlemler, yapılabilecek geliştirmeler
* Deployment of a Flexible Malware Sandbox Environment Using Open Source Software 01.01.2015 Jose Ortiz Sandbox'ta yapılacak çalışmaların otomatize edilmesi ve ölçeklendirilebilmesine yönelik geliştirmeler

**Yöntem**

**Başarı Ölçütü**

Hedeflenen Değer 2015 yılına kadar olan literatürden rastgele seçilen zararlı yazılımın tespit edilebilmesi

100 adet zararlının 80 tanesinin tespiti %80

2016 yılında karşılaşılan rastgele seçilen zararlı yazılımın tespit edilebilmesi

10 adet zararlıdan 7 tanesinin tespiti - %70

Sistem kapasitesi ve ölçeklenebilirliğinin sağlanması 20 adet analizi eş zamanlı (anlık) gerçekleştirme API'nin popüler güvenlik denetim kaynaklarından aktarım yapabilmesi, aktarımın sağlıklı çalışması

En az 4 farklı kaynak (marka)

Sanal Makina Sandbox Yazılımı (Bir işletim sistemini taklit eden, sıradan bir kullanıcı bilgisayarını andıran ancak daha küçük boyutta olan sanal bir yazılım olup, bu ortamın ilk anki haline döndürülmesi, başa alınması ve işlemin tekrarlanması oldukça kolaydır. Zaten geliştirilen tüm bu sistemin amacı da zararlı yazılımlar üzerinde hızla deneme yapılabilecek, işlemin tekrarlanabileceği bir yapının hızlıca oluşturulmasına yöneliktir.)

- Sanal makine atlatma yöntemleri, tersine mühendisliği tespit tekniklerinin gözden geçirilmesi, sanal makine atlama, - Yüksek miktarda analiz aktarabilme ve büyük veri (big data) raporlamaya yönelik geliştirilecek metotlar

- API geliştirmeleri ile diğer sistemler ile iletişim sistemi üzerine çalışmalar yapılacaktır. Geliştirilen kum havuzunun çalışma düzeyi deneysel metot ile test edilecektir; oluşturulan kum havuzu içerisine özellikleri bilinen zararlı yazılım aktarılacak, sistemin zararlı yazılımın yapmaya çalıştığı bilinen izinsiz ve zararlı hareketlerinin tespiti için, hangi tespit yöntemlerinin başarılı olduğu, tespit yöntemlerinden hangilerinin yetersiz kaldığı incelenecektir.

Farklı karakteristik özelliklere sahip zararlı yazılımlar için deneyler sürdürülerek, bilinen mevcut metotlara karşı başarı oranı artırılacaktır. İncelemeler sonucunda başarısız bulunan tespit metotlarının geliştirilmesine yönelik çalışma yapılacaktır.

Zararlı yazılımlar tarafından kum havuzu (sandbox)nun tanınmaması üzerine örtüleme ile sistemlerin güçlendirilmesi

- Mevcut uygulamalardaki sistem çağrı takibi (syscall trace) yerine farklılık inceleme (diff) metodu ile zararlı yazılımın hareket takibi

- Kullanıcı hareket simülasyonu ile gerçek kullanıcı taklidinin yapılması

**Diğer öneriler**

ISR fuzzer ile Genetik algoritması

Bulut Tabanlı Ölçeklenebilir Kum Havuzu (Central Sandbox Inspection)

Mevcut teknolojiler ile tespit edilemeyen zararlı yazılımları tespit yeteneğine sahip ağ güvenlik cihazının (donanım-yazılım bütünleşik, yazılım geliştirilerek) üretilmesi.

Bu proje ile zararlı yazılımların bulut teknolojisinin düşük maliyet ve yüksek ölçeklenebilirlik avantajlarına sahip olan merkezi kum havuzu üzerinde incelenmesi, zararlarının tespit edilmesi ve raporlanması sağlanmaktadır.

Proje ile mevcut altyapılardaki güvenlik eksikliğinin giderilmesi, statik bazlı analizler ile sınırlı olan, kum havuzu (sandbox) teknolojileri olmayan mevcut eski güvenlik duvarları, antivirüs yazılımları gibi teknolojilerin tespit edemediği zararlı yazılımların tespitini sağlamak üzere CSI sistemine API ve istemci (client) ile aktarılması, entegre olması ile dinamik analiz becerisinin getirilmesi, sistemden veri çalma veya veriye zarar verme hedefi olan zararlıların eski teknolojilerde de tespitinin mümkün kılınması üzerine çalışılacaktır.

Ayrıca oluşan bu zararlı yazılım veri tabanı ile ülke güvenliğinin sağlanmasına yönelik veri toplanması, en sık karşılaşılan saldırılara karşı önlem alınması da mümkün olacaktır.