Bilgi Sistemleri ve Güvenliği Final Projesi Dokümantasyonu

Proje Ekibi

16542005 - Alperen Şişman

2021

1. Giriş

Keylogger, bilgisayarda yaptığınız her işlemin kaydını tutarak verilerinizi çalmak isteyen art niyetli kişilere gönderen bir casus yazılımdır. İlk önceleri sadece bastığınız klavye tuşlarını kaydedebilen bu yazılımlar, artık bilgisayar üzerinde hemen hemen her yaptığınız işlemi karşı tarafa iletebiliyor. İlk keylogger uygulamaları 1970'li yıllarda Sovyetler Birliği'nde ortaya çıkmıştır[2]. O zamanlar genel iletişim yöntemi elektrikli daktilolar tarafından yazılan mektuplardı ve istihbarat örgütleri bu bilgilerin peşindeydi. Sovyet ajanları ABD büyükelçilerinden bilgi elde edebilmek için, ABD'li diplomatların istihbarat amaçlı kullanmış oldukları IBM Selectric adındaki daktilolara yazıcı kafasının üzerindeki şeritleri kaydeden bir donanım yerleştirmişlerdi. Bu sayede yazılan her veri, yazıcı kafasına kaydediliyor ve sonrasında istihbarat birimlerine iletilerek okunabiliyordu. Sovyet ajanlarının gizli bilgi edinme çabaları elbette ki bununla sınırlı değildi. Ayrıca ABD Büyükelçilik binalarının duvarlarına gizlenen donanım tabanlı keyloggerlar da bu yıllarda kullanılmıştır. Başlıca keylogger türleri aşağıdaki gibidir[1];

I. Çekirdek tabanlı keyloggerlar; İşletim sistemi altında çalışan ve en tehlikeli türlerden biridir. Bu türe karşı alınabilecek önlemler maalesef ki sınırlıdır. Kök erişimi elde ettikleri için tespit edilmesi de çok zordur. Bu türdeki keyloggerlar çekirdek erişimi için rootkit kulanır ve genellikle donanımlara yetkisiz erişim elde ederek işlevlerini yerine getirir.
II. Yönetici tabanlı keyloggerlar; İşletim sistemi altında hipervizör katmanında çalışan keylogger türlerinden biridir. Etkilidir ve bir sanal makine olarak çalışmaktadır.
III. Api tabanlı keyloggerlar; İşletim sistemi API'lerine erişim sağlayarak çalışan bu türdeki keyloggerlar işletim sisteminin algıladığı tüm tuş girişlerine bir kanca atarak kopyalamaktadır. Bellekte kalan doğrulama PIN kodlarınızdan BIOS sorgulamasına kadar birçok alanda aktiftirler.
IV. Form tabanlı keyloggerlar; Yalnızca form verilerini kaydetmek ve web formlarında araya girmek amaçlı üretilmişlerdir. Bir kayıt formundan giriş formlarına kadar her türlü formu dinleyebilme ve bu formlardan gönderilen tüm verileri kopyalayabilme yeteneklerine sahiptirler. Bu türlerin geneli Web uygulamalarına yöneliktir.
V. Javascript tabanlı keyloggerlar; Web uygulamalarındaki kullanıcı bilgilerini çalmaya yönelik keyloggerlardır. Bir web sayfası hacklenerek zararlı bir kod enjekte edilir. Bu sayede web sayfasına girip işlem yapan herkesin klavyede bastığı tuşlar kaydedilerek hesap bilgileri çalınmaktadır.
VI. Bellek tabanlı keyloggerlar; İşletim sistemlerine bulaştıklarında kendilerini bellekte çalıştıran, bellekte yer alan tüm uygulamaları izleyerek bilgi çalmayı hedefleyen keylogger türüdür. Bellekte çalıştıkları için iz bırakmazlar ve tespit edilmeleri zordur. Genel olarak Windows tabanlı bilgisayarlarda işletim sisteminin bir güvenlik mekanizması olan UAC'yi atlatmayı amaçlamaktadır.

2. Uygulama Süreci

Bulaşma yolu spam mail internet siteleri üzerindeki açılır reklamlar veya internet üzerinden indirdiğiniz orijinal olmayan sistem dosyaları vb. şeklindedir. İndirilen bu dosyalar aracılığı ile bu casus yazılım karşı tarafa size ait olan şifreler, dosyalar, görüntüler vb. birçok dijital nesneyi aktarır. Bu projede karşı tarafın klavyesi dinlenecektir.

2.1 Uygulama Aşamaları

Oluşturulacak keylogger casus yazılımının aşamalarını 3 başlıkta gösterebilriz. Bunlar;

- Karşı tarafa casus yazılımın bulaştırılması,
- Casus yazılımın hedef sistemi dinlemesi,
- Casus yazılımın dinlediği klavye girdilerini hackera(beyaz ve ya siyah) göndermesi.

Casus Yazılı Hedef Sisteme Bulaştırmak

Bir casus yazılımı hedef sisteme bulaştırmanın birçok yolu olabilir. Bu yolları uygulamadan önce bilinmesi gereken bir detay var. Bu detay ise hedef sistemde antivirüs sistemlerinin olmaması veya çalışmamasıdır. Hedef sisteme casus yazılımı bulaştırmanın yollarından bazıları;

- Sosyal Mühendislik
- Sahte Web Uygulamaları
- Hedefin Dikkatini Çekebilecek E-Postalar
- Hedef Sisteme Doğrudan Bulaştırmak

Hedef Sistemin Dinlenmesi

Casus yazılımın hedef sisteme bulaştırılması aşamasını başarıyla geçtikten sonra, geliştirdiğimiz keylogger casus yazılımının hedef sistemi dinlemesi aşamasına geliyoruz. Bu aşamada casus yazılımımız, hedef sistem her kapatılıp açıldığında kendi kendini yeniden başlatması gerekiyor. Hemen ardından casus yazılımımızın tespit edilememesi çok önemlidir. Bunu sağlamak için yazılımımızı arka planda çalışabilecek şekilde tasarlamamız gereklidir. Hedef sistemin kullanıcılarının klavyeden girdikleri her bir girişi, casus yazılımımız kontrol etmeli ve bu girdilere karşılık gelecek karakterleri ram bölgesinde kaydetmeli. Bunun için static yapıda bir değişken yeterli olacaktır.

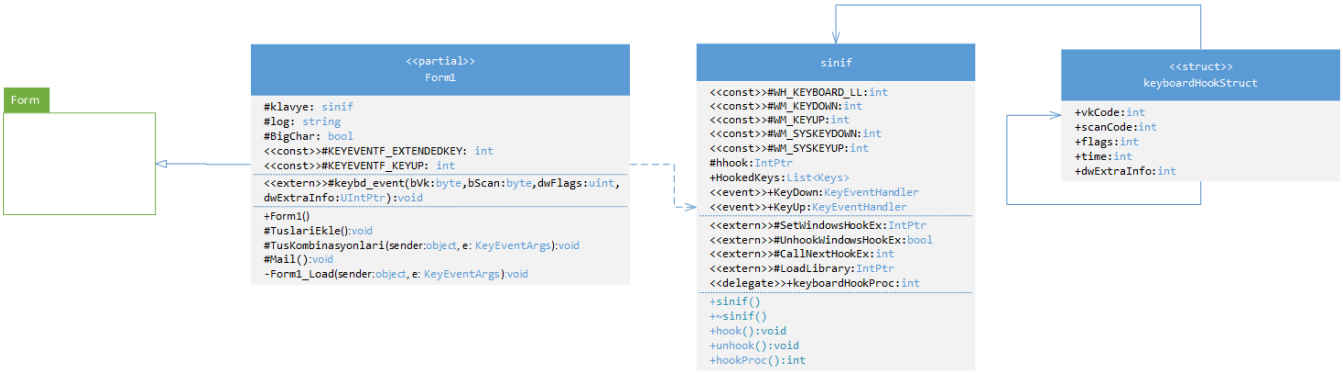
Kaydedilen Girdilerin Hacker'a Gönderilmesi

Hedef sistem girdilerinin yine hedef sistemde saklı tutulması casus yazılım mantığının dışında kalacaktır. Bu nedenden dolayı ram bölgesinde tutulan hedef sistem girdilerini hacker'a 2 yöntem ile gönderebiliriz. Bu yöntemler;

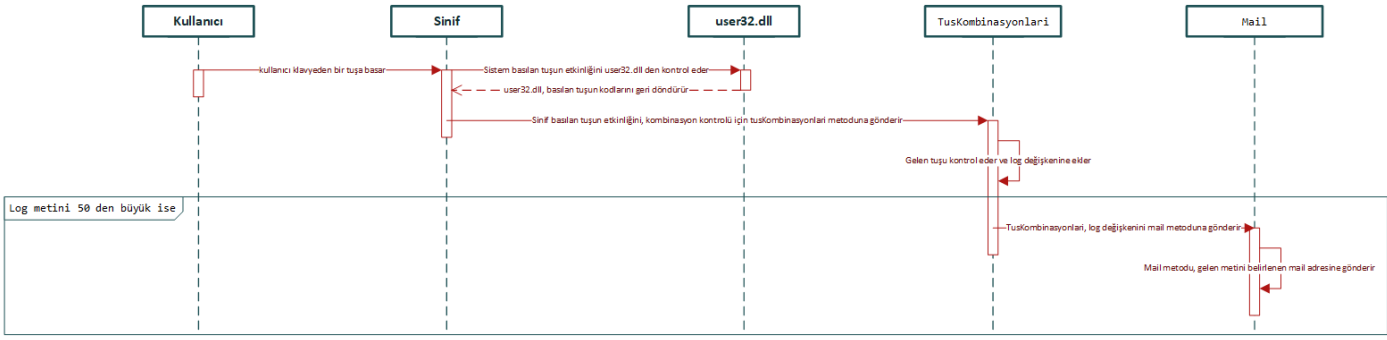
- Simple Mail Transfer Protocol(SMTP)
- Uzak Sunucuya Kaydetmek(DNS)

Uzak sunucuya verileri göndermek için bir tane çalışır web sitesi yeterli olacaktır. Sahip olunan domaine "_GET" işlemi ile bu verileri gönderebiliriz. Bu projede kullanacağımız yöntem ise SMTP yöntemidir. Bu protocolde ram bölgesindeki verileri alıp doğrudan kendi mail adresimize gönderim sağlayabiliriz. Gönderim işlemi başarılı olduktan sonra ram bölgesinde tuttuğumuz verileri sıfırlamamız gereklidir.

Diyagramlar



Şekil 1 Sınıf Diyagramı



Şekil 2 Sequance Diyagramı

3. Uygulama Sonucu

Projemizinde test sistemi olarak Windows 10 işletim sistemi seçilmiştir. Geliştirilen casus yazılım bu sisteme bulaştırılıp sonuçlar gözlenmiştir. Gözlemler sonucunda kullanıcı olarak sahip olunan klavyeye girdiler verilip, uygulamanın etkinliği izlenmiştir. Casus yazılım 50 karakter uzunluğuna ulaştığında STMP protocolü ile kendi e-posta adresimize, dinlediği girdileri göndermiştir.

4. Kaynakça

[1] https://berqnet.com/blog/keylogger

[2] https://tr.wikipedia.org/wiki/Klavye_dinleme_sistemi