

Flash Player'da Güvenlik

Kendi kendine yetebilmek hayatın birçok alanında önemli bir kazanım olarak karşımıza çıkmaktadır. Bağımsız karar verebilmenin, rahat ve özgürce hareket edebilmenin de ilk koşulu kendi kendine yetebilmek değil midir? Yazılım dünyasında da aynı yaklaşımı görebilmek mümkündür. Çalıştırılabilen (executable) dosyalar her zaman dağıtım ve kullanım açısından avantaj sağlamıştır.

90'ların başında, henüz İnternet ve çoklu ortam aygıtları ile tanışmadığımız dönemlerde, bilgisayarların dış dünya ile kurdukları ilişki manyetik disklerden ibaretti. İletişim (com port) kapılarının yegane kullanıcıları ise farelerdi. Bilgisayarımıza yapılabilecek harici bir saldırı ya disket sürücüden gelen virüslü bir uygulama olabilirdi yada bir doğal afet (su baskını, yıldırım, yüksek gerilim vs..).

Virüs konusunda ise belirli kriterler vardı. Günümüzdeki gibi zengin bir portföy yoktu Hacker'ların elinde. *.exe, *.com, ve *.bat uzantılı dosyalar şüpheliler listesinin başındaydı. Bu dosyaları tehlikeli yapan kendi kendilerine çalışabiliyor olmalarıydı. Gelişen bilgisayar terörizmi Hacker'lara, makro virüslerinden truva atları (trojan) ve solucanlara (worms) kadar geniş bir cephe açtı. İnternet gibi geniş alan ağlarıyla kıtalar arası rahatça seyahat edebilen bu virüsler, yerel alan ağları sayesinde ise süratle yayılmaya başladılar. Artık kapatılması yada denetlenmesi gereken birçok iletişim kapısı (com port) ve taranması gereken birçok dosya tipi bulunmaktaydı. Bütün bu değişim esnasında değişmeyen tek şey, *.exe, *.com, ve *.bat uzantılı dosyaların yarattığı tedirginlik oldu belki de. Özellikle bu dosya uzantılarına sahip dosya ekleriyle gelen e-postalar okunmadan silinmeye başlandı. Outlook gibi gelişmiş e-posta uygulamaları ise bu tür postaları bloke etmeyi bir çözüm olarak gördü.

Sunucu bilgisayarların yada internet üzerinde gerçek ip alabilen kullanıcıların (dial-up yada kablolu aboneler) sistemlerindeki boşluklardan faydalanan Hacker'ler truva atlarını sabit disklere kolayca yerleştirmeye başladılar.

Flash'ın popülaritesinin sürekli artması, kullanıcıların bu uygulamaya karşı güvenlerini de arttırmaktaydı. Flash filminin exe haline getirilebilmesi ve tüm

materyallerin bu *.exe uzantılı dosya içine gömülebilmesi dağıtımını da kolaylaştırmaktaydı. Beşinci versiyonu ile eskiye göre kodlama yeteneği hayli artan Flash, oynatıcısının yaygınlığı ile de geliştiricilere zengin bir uygulama alanı sunmaktaydı.

ActionScript içinde yer alan FS Command'ler yardımı ile sistemde yer alan *.exe ve *.bat uzantılı dosyaları çalıştırılabiliyordu. Flash Player 5'in bu yeteneği uygulama geliştiriciler için faydalı bir özellikti. Bu özellik kötü amaçlı kullanımlara da fırsat verebilirdi. Zararlı bir uygulamayı tetikleyebilir yada kullanıcının isteği dışında sistemle ilgili servisleri açıp kapatabilirdi. Bu tür bir olasığın varlığı henüz karşılaşılan önemli bir sorun olmasa da kullanıcıların Flash Player'a karşı olan güvenlerini sarsabilirdi.

FS Command kodlarının, Flash uygulaması Projector (*.exe) haline dönüştürülmese de çalışabiliyor olması endişelerin bir kat daha artmasına neden olmuştu. Bu durumda *.swf uzantılı olarak gelen bir dosya başka uygulamaların tetikleyicisi olabilirdi. İnternet üzerindeki Flash içeriğinin Temp dizinine yerleşmesi ve bu dizin içinde FS Command'in "exec" fonksiyonunun işlevsiz kalıyor olması kullanıcıları bir parça rahatlattı.

Flash MX'le beraber kullanıma giren Flash Player 6'da tüm bu güvenlik açığı olarak yorumlanabilecek uygulama seçenekleri devreden çıkartıldı. Yeni haliyle FS Command içinde yer alan "exec" fonksiyonu artık *.bat uzantılı dosyaları çalıştıramaz hale getirilmişti. *.exe uzantılı bir dosyayı çalıştırabilmesi için de kendi dizini içinde "fsccommand" isimli bir klasör yaratılması gerekmekteydi. Çalıştırılacak exe dosyası bu klasörün içinde yer almak zorundaydı. Bu şartlara bir de tetikleyici dosyanın Projector (*.exe) olması koşulu da eklendi. Artık SWF halindeki Flash Filmleri "exec" fonksiyonunu çalıştıramıyorlardı.

Bu durum akla hemen bir atasözünü getirmektedir. "Kurunun yanında yaş da yanar". Gerçektende bir çok uygulamada kullanılabilecek önemli bir özelliğin devreden çıkarıldığını görüyoruz. Yaş olan bizler, (tuzu) kuru Hacker'ler yüzünden bir kere daha güvenlik önlemlerinin engeline takılıyoruz.

R. Orçun Madran