Salı Sallanır

written by Mert SARICA | 27 July 2010

Patch Tuesday yani her ayın 2. Salı günü, Microsoft firması tarafından ürünlerine ait güvenlik yamaları yayınlanır. Kimileri için bu yamalardan bazıları bilgisayarın yeniden başlatılmasını gerektirdiği için can sıkan gereksiz güncellemelerken, kimileri için test edilmesi ve daha sonra istemci işletim sistemlerine kurulması gereken çileli bir iş yükü demektir. Fakat kimileri içinse bu gün kazanç kapısını aralamak anlamına gelir.

İstemci taraflı uygulamalardaki (örnek: winzip, adobe reader, winrar vb.), işletim sistemlerindeki güvenlik zafiyetlerini istismar etmeye yarayan istismar paketlerini (örnek: MPack, CRiMEPack vb.) geliştiren art niyetli kişilerin amaçları yayınlanan güvenlik zafiyetini istismar eden kodu derlemek ve paketlerini güncellemektir. Güncellenen her paket yeraltı dünyasındaki müşterilerine pazarlayacakları yeni bir sürüm olduğu için 2. Salı günü yayınlanan yamalar üzerinde hummalı bir çalışma başlar.

Bu çalışma için öncelikle bu kişilerin bu yama ile güncellenen paketi tespit etmeleri gerekmektedir. Microsoft Destek sayfası bu bilgiyi edinmek için en kolay ve zahmetsiz yoldur. Örneğin bu sayfada MS10-005 anahtar kelimesini aratacak olursanız karşınıza çıkan sonuçlarda yer alan sayfalarda bu yama ile hangi dosyanın (yazılımın kendisi olur veya ilgili DLL dosyası olur) güncellendiği bilgisine kolayca erişebildiğinizi göreceksiniz.

Windows XP'nin tüm desteklenen x86 tabanlı sürümleri

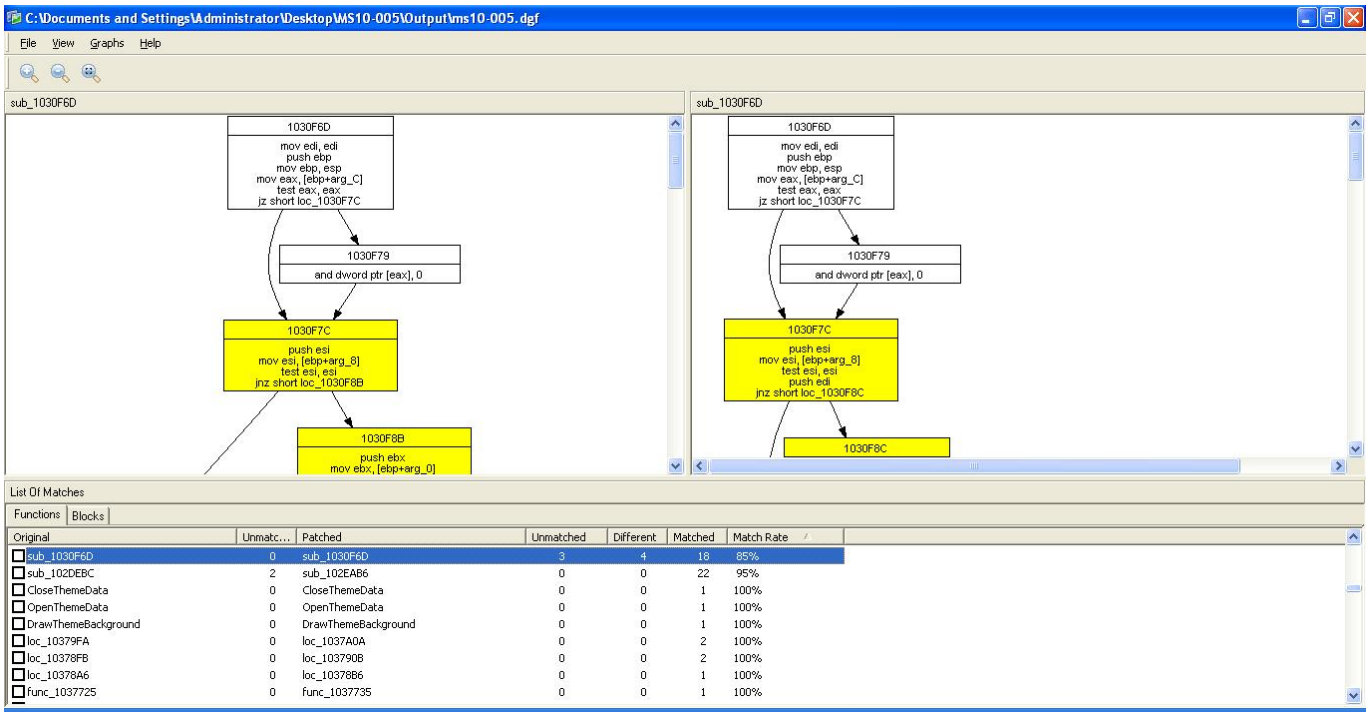
File name	File version	File size	Date	Time	Platform	SP requirement	Service branch
Mspaint.exe	5.1.2600.3660	343,040	16-Dec-2009	12:58	x86	SP2	SP2GDR
Mspaint.exe	5.1.2600.3660	343,040	16-Dec-2009	13:37	x86	SP2	SP2QFE
Mspaint.exe	5.1.2600.5918	343,040	16-Dec-2009	18:43	x86	SP3	SP3GDR
Mspaint.exe	5.1.2600.5918	343,040	16-Dec-2009	18:27	x86	SP3	SP3QFE

Paketi tespit ettiler peki ya sonra ? Daha sonra yapmaları gereken ise programın (mspaint.exe) güncellenen sürümü ile eski sürümünü assembly seviyesinde karılaştırmak ve farkları ortaya çıkarmak olacaktır. Yama geçilmiş bir Windows işletim sistemi üzerinde yazılımın eski sürümünü elde etmek için ilgili yamayı denetim masasındaki program ekle/kaldır menüsünden

kaldırarak elde edebilirsiniz. Tabii yamayı kaldırmadan önce güncel yazılımın bir kopyasını almayı unutmayın.

Yamayı kaldırdıktan sonra eski sürüm ile yeni sürümü kıyaslamak için yaygın olarak kullanılan ücretli ve ücretsiz 3 programdan faydalanmaktalar. Bunlar sırasıyla, Zynamic'in BinDiff (ücretli), eEye'in DarunGrim, Tenable'ın PatchDiff programlarıdır. Bu üç programda IDA Pro yazılımının eklentisi olarak çalıştıkları için IDA PRO'nun mutlaka işletim sistemi üzerinde kurulu olması gerekmektedir. 3 programında çalışma mantığı birbiri ile hemen hemen aynı fakat DarunGrim yazılımının daha anlaşılır olduğunu not olarak belirtmek isterim.

Hangi programı kullanırlarsa kullansınlar bu programlar sayesinde yama ile hangi fonksiyonda değişiklik yapıldığını tespit etmeleri çok uzun sürmez. Bunun için yapmaları gereken DarunGrim yazılımında File menüsünden New Diffing from IDA'yı seçmek ve Source için eski sürümü, Target için yeni sürümü ve Output için ise herhangi bir klasörü belirtmek yeterli olacak ve DarunGrim gerisini halledecektir. Analiz tamamlandıktan sonra DarunGrim size eski sürüm ile yeni sürümde yer alan her bir fonksiyon için eşleşme değerini (Match Rate) gösterecektir. %100 eşleşen bir fonksiyonun değişmediğini daha az yüzdeler ise fonksiyonda değişiklik olduğunu işaret etmektedir. Kontrol akışı izlendiğinde sarı renk bir eski sürüm ile güncel sürüm arasında bu bloğun değiştiğini, kırmızı ise yeni bir blok eklendiğini belirtmektedir.



Son olarak assembly kodunu dikkatlice inceleyerek hatalı, zafiyet barındıran

kodu tespit eden bu kişiler istismar aracını geliştirdikten sonra derleyerek paketlerine eklerler. Yamasını geçmeye üşenen kişiler/kurumlar ise gün geçmeden art niyetli kişilerin hedefi olurlar. Siz siz olun her ayın 2. Salı günü zamanla yarışan art niyetli kişilerin hedefi olmamak için işinizi gücünüzü bir kenara bırakarak güvenlik yamalarını geçmeye bakın…