Kanald Vaka-i Analiz

written by Mert SARICA | 30 April 2010

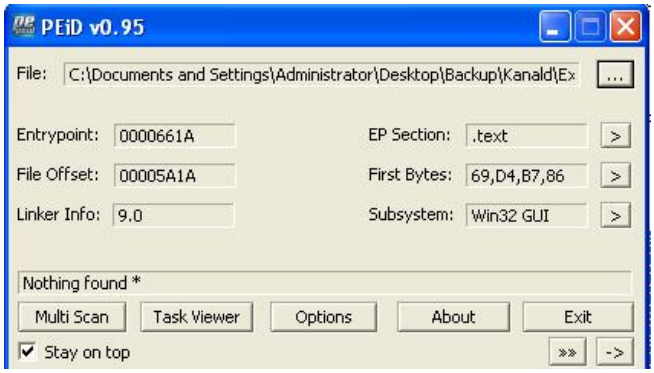
Hatırlarsanız geçtiğimiz hafta bilgisayar korsanları Kanald web sitesini hacklemişler, bende şans eseri o esnada web sayfasını ziyaret eden biri olarak olaya tanık olmuş ve doktor iyileşecek hastanın ayağına gidermiş misali hemen verileri toplayarak analiz etmeye ve insanları konu ile ilgili bilgilendirmeye çalışmıştım. Yaptığım kısa bir analiz çalışması sonucunda bilgisayar korsanlarının Kanald web sitesini ziyaret eden ziyaretçileri kendi sitelerine yönlendirmelerindeki asıl amaçlarının sitelerine koydukları internet explorer istismar kodu ile ziyaretçilerin sistemlerini ele geçirmek ve tuş kaydı yazılımı yüklemek olduğu ortaya çıkmıştı.

Peki kısa bir sürede nasıl böyle bir sonuca varmıştım, kısaca açıklayayım.

Öncelikle sayfanın kaynak kodlarına baktığımda metasploit istismar kodlarına zaman zaman göz atan biri olarak internet explorer yazılımını hedef alan bir kod olduğunu anlamam pek zor olmadı. Hemen ardından acaba bu girişim ile hedef sistem üzerinde korsanlar ne yapmak istiyorlardı sorusuna yanıt aramaya koyulmuşken 37 kb boyutunda binary formatındaki uzayıp giden son satır dikkatimi çekiverdi.

value="4d5a90000300000004000000ffff0000b800000000000000400000000000000000000000000000000000000000000000000000000000000000000000e00000000e1fba0e00b409cd21b8014ccd21546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64652e0d0d0a2400000000000000eb9a4632affb2861affb2861affb2861b1a9ac61b5fb2861b1a9bd61bffb2861b1a9ab61e6fb2861883d5361acfb2861affb2961e6fb2861b1a9a261aefb2861b1a9b961aefb286152696368affb2861000000000000000000000000000000000000050450000 04c010400884a2b4b..."

İlk işim binary formatındaki bu kodu hex editör ile exploit.exe adı altında kayıt etmek ve incelemek oldu. Genellikle bu ve benzer kötü niyet güden programlar ya paketlenmiş ve/veya şifrelenmiş olurlar bu nedenle hex editör ile incelediğimde ipucu adına pek fazla birşey bulamayacağımı düşünüyordum. Minimum 5 karakter olarak ASCII ve UNICODE olarak stringleri tarattığımda anlamlı olabilecek yaklaşık 100 tane string ile karşılaştım. 37 kb boyutunda bir binary ve yaklaşık 100 tane string ? Aklıma pek yatmadığı için biraz kuşkuyla yaklaştım ve PEID ile emin olmak için exploit.exe yazılımını inceledim, sonuç paketlenmemişti.



Bu işte bir iş var diyerek birde Immunity Debbuger ile exploit.exe yazılımını incelemeye karar verdim. Kısa bir incelemeden sonra yazılımın çalışma esnasında içerisinde şifrelenmiş olarak tutulan kod parçacıklarını, 0x1000 byte boyutundaki 0x00390000 bellek alanına kopyaladığını ve XOR ile şifrelenmiş kod parçacıklarını çözdüğünü gördüm. Çözme işlemini kısa bir süre takip ettikten sonra ortaya http://217.23.7.125/xxx.exe web adresi çıkıverdi. Bu web adresi, exploit.exe adı altında kayıt etmiş olduğumuz bu zararlı yazılımın bir trojan downloader olduğunu ve ana zararlı yazılımı yani tuş kayıt yazılımını, içerisine gömülü olan bu web sitesinden indirerek çalıştırmak üzere tasarlandığı anlamına geliyordu.

Haliylen bu zararlı yazılımın otomatik olarak tuş kayıt yazılımını bu web sitesinden indirip kurmasına göz yumamayacağım için manuel olarak xxx.exe yazılımını indirip hex editör ile incelemeye ve stringlere göz atmaya başladım. Kısa bir inceleme sonucunda bu yazılımın leetlogger adında bir tuş kayıt yazılımı olduğu ortaya çıktı ve dinamik analize gerek kalmadı.

Uzun uzun yazılar okumaktansa video izlemeyi her zaman tercih eden ve bu nedenle yazılarımda olabildiğince videolara yer vermeye çalışan ve sizede ister istemez bu alışkanlığı kazandırmış biri olarak yaptığım analizi özetleyen 4 dakikalık ufak bir video hazırladım, herkese iyi seyirler dilerim.