AutoIt Hata Ayıklaması

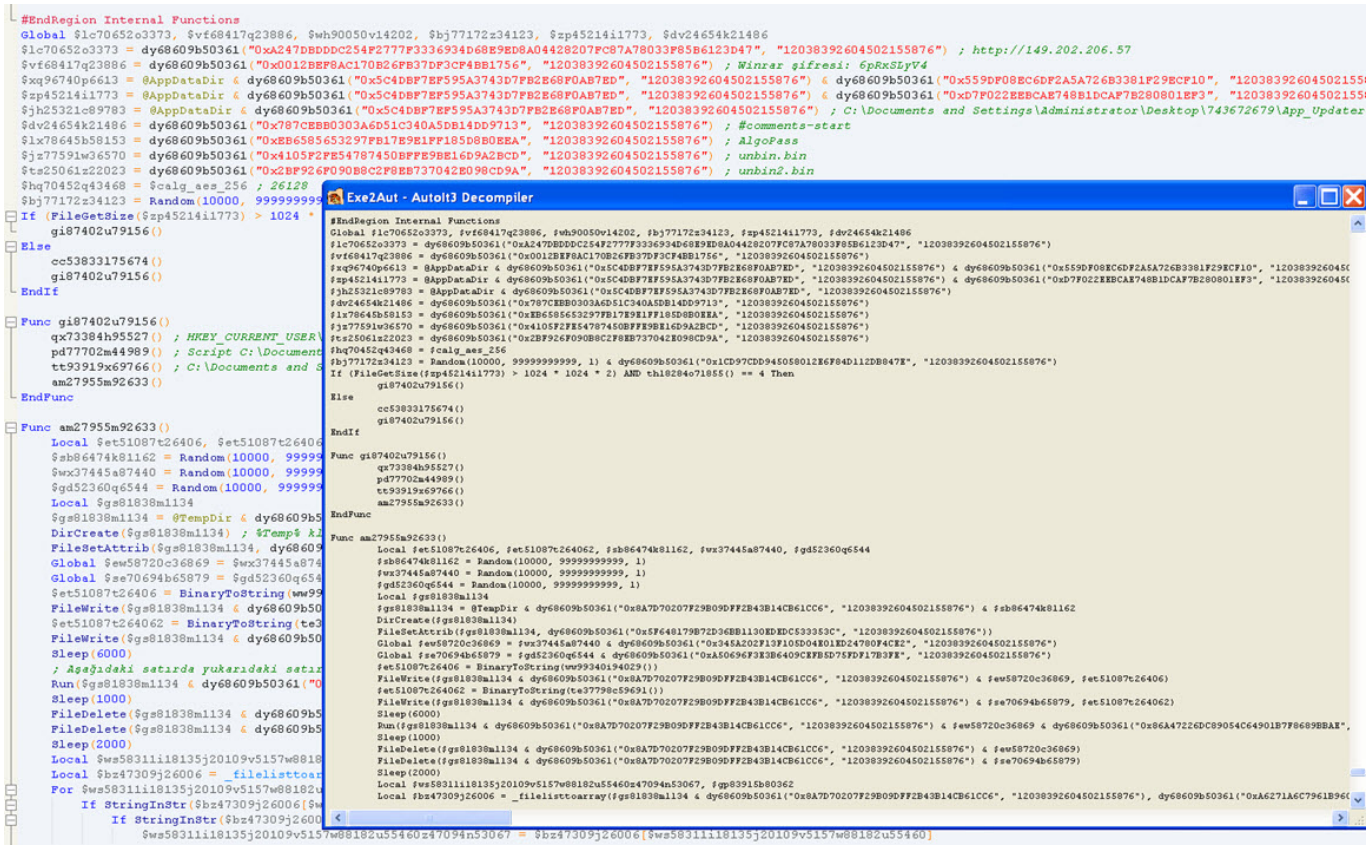
written by Mert SARICA | 1 February 2017

Hem Pi Hediyem Var oyununun altıncısına hem de AutoIt Bankacılık Zararlı Yazılımı başlıklı blog yazıma konu olan zararlı yazılımı/betiği incelediğimizde, AutoIt'in son yıllarda zararlı yazılım geliştiriciler tarafından sıklıkla kullanıldığını görebiliyoruz. APT gibi hedeflenmiş siber saldırılarda da AutoIt ile geliştirilmiş zararlı yazılımların kullanılıyor olması, zararlı yazılım analistleri ve zararlı yazılım analizi becerisine sahip siber güvenlik uzmanları tarafından analiz edilebilmesini ihtiyaç haline getirmektedir.

Wikipedia'dan alıntı yapacak olursak, "AutoIt, Microsoft Windows için ücretsiz bir otomasyon yazılımıdır. Yazılımın ilk versiyonları tamamen otomasyona yönelik hazırlanmış olsa da sonradan kapsamı genişletilerek hemen her türlü uygulamanın geliştirilebileceği bir programlama aracı haline gelmiştir. Bir AutoIt betiği, AutoIt yorumlayıcısının yüklü olmadığı bilgisayarlarda çalışabilecek şekilde, sıkıştırılmış bir EXE programı haline getirilebilir."

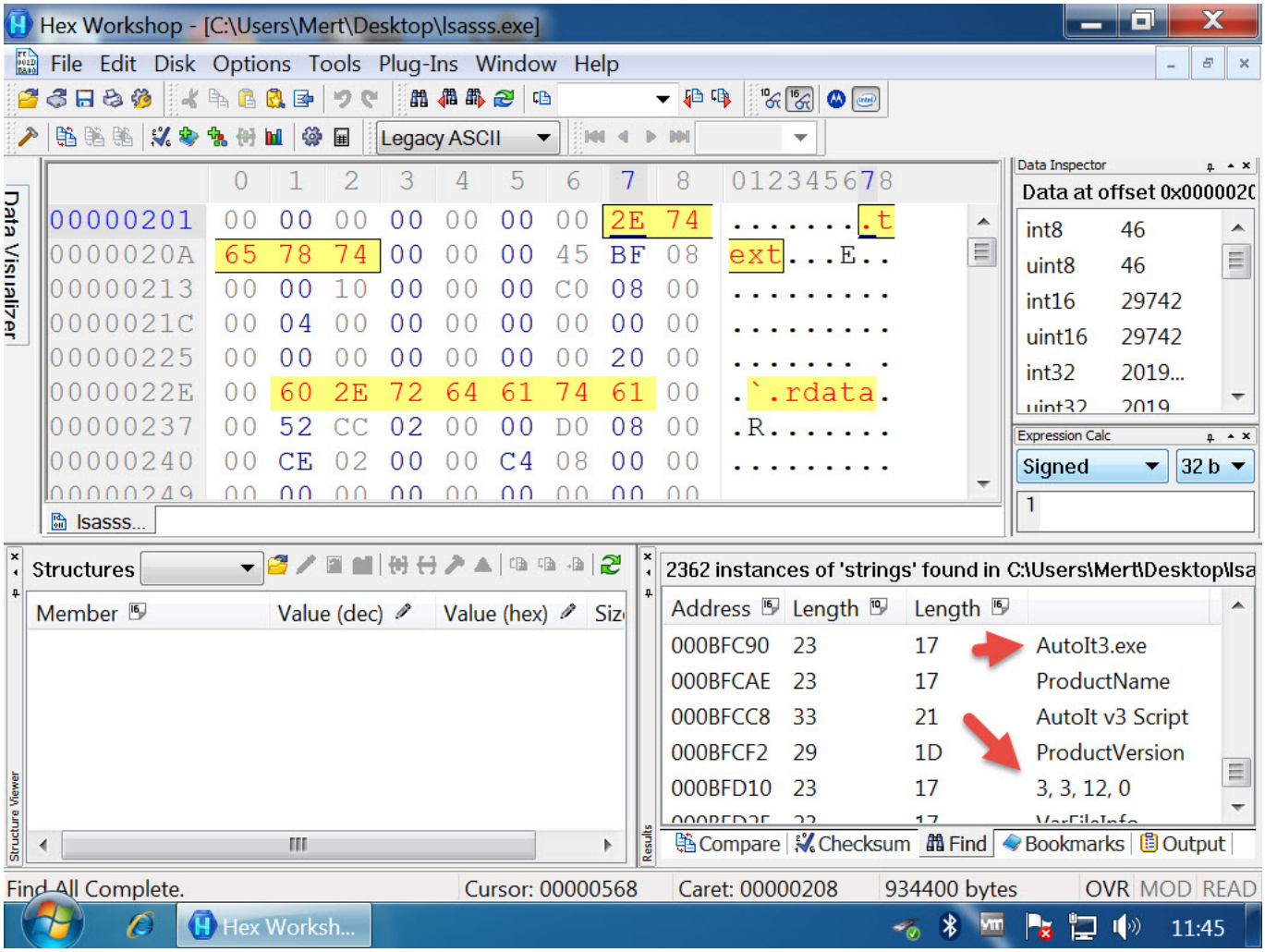
Eğer "AutoIt Bankacılık Zararlı Yazılımı" başlıklı blog yazımdaki gibi şanslıysak, elimizdeki AutoIt betiğini (script) çeşitli hata ayıklama (debug) araçları ile analiz edebiliriz. Eğer derlenmiş, exe uzantılı bir AutoIt dosyası ile karşı karşıya isek bu durumda yapacağımız ilk iş, derlenmiş AutoIt dosyasını, betiğe çevirmek olacaktır.

Derlenmiş AutoIt dosyasını betiğe çevirmek için Exe2aut aracından faydalanabiliriz. Exe2aut aracını çalıştırdıktan sonra exe uzantılı AutoIt dosyasını araca sürükledikten sonra betik dosyasına kolaylıkla ulaşabiliyoruz.



Peki betiğe ulaştık, şimdi ne yapacağız ? AutoIt'in web sayfasında yer alan Sıkça Sorulan Sorular sayfasına bakacak olursak, hata ayıklama için çeşitli araçlardan faydalanabileceğimizi görebiliyoruz.

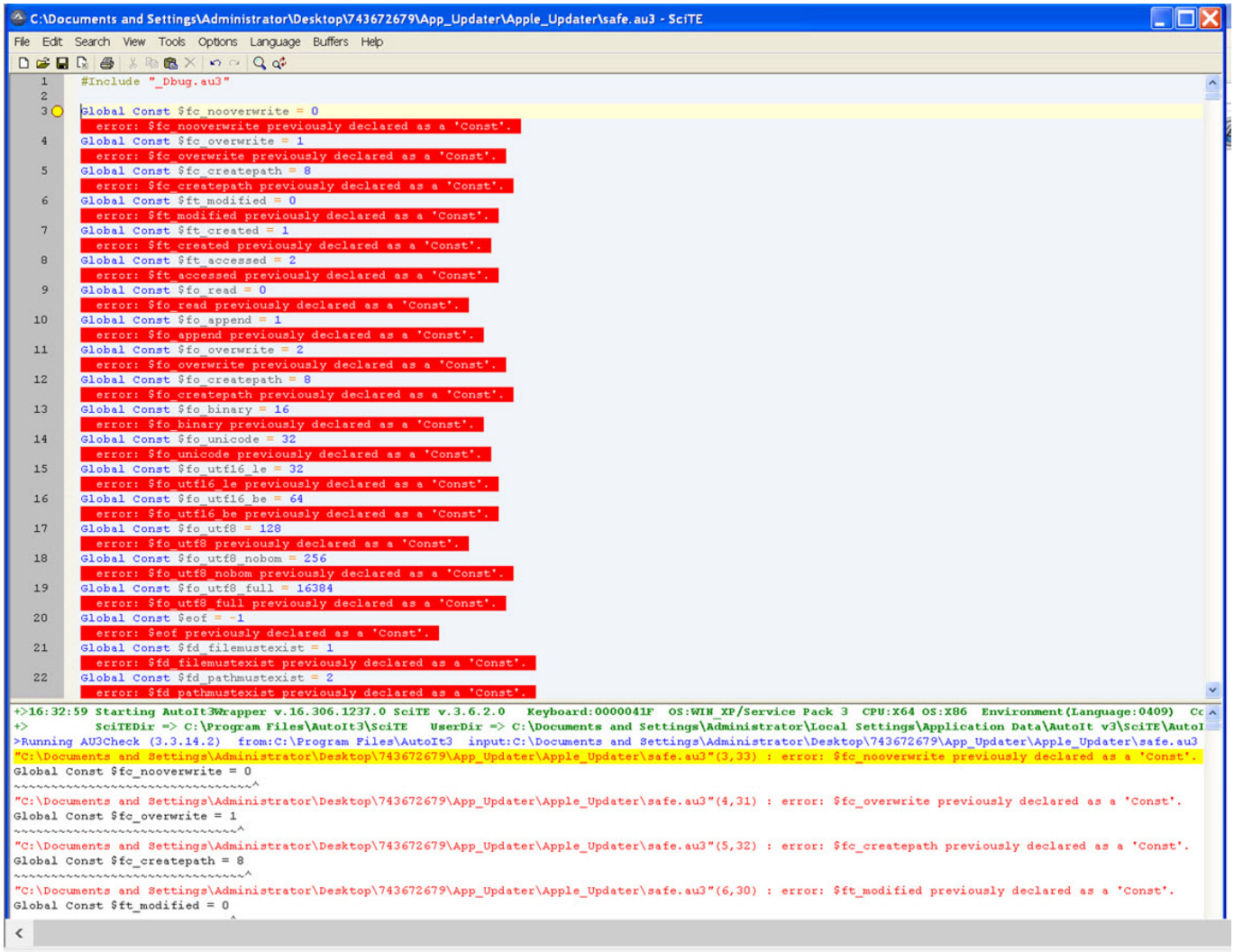
6. Pi Hediyem Var oyununda kimilerinin safe betiğini analiz ederken hata ayıklama araçları yerine ConsoleWrite(), MsgBox() gibi ekrana değişkenlerin sahip olduğu değerleri yazmak için kullanılan fonksiyonlardan faydalandığını gördüm. Her ne kadar bu da bir yöntem olsa da işleri kolaylaştırmak ve daha hızlı ilerlemek için hata ayıklama araçlarından faydalanmanızı tavsiye ederim. Tabii kimi zaman hata ayıklama araçlarıyla sorun yaşamanız da olasıdır. Örneğin yine 6. Pi Hediyem Var oyununda, hata ayıklama araçlarından olan Dbug aracını AutoIt programının son sürümü ile kullanarak safe betiğini analiz etmeye çalışanlar, #comments-start ile #comments-end takıları arasında yer alan gizlenmiş (obfuscated) verilerin hatalı olarak çözülerek diske yazıldığına şahit oldular. Bu ve benzer sorunlarla karşılaşmama adına, zararlı yazılımın geliştirildiği AutoIt sürümü ile betiği analiz ederseniz, sorun yaşama ihtimaliniz oldukça düşecektir. AutoIt sürümünü bulmak için ise betik ile birlikte gelen AutoIt programının karakter dizilerini (strings) incelemeniz yeterli olacaktır.



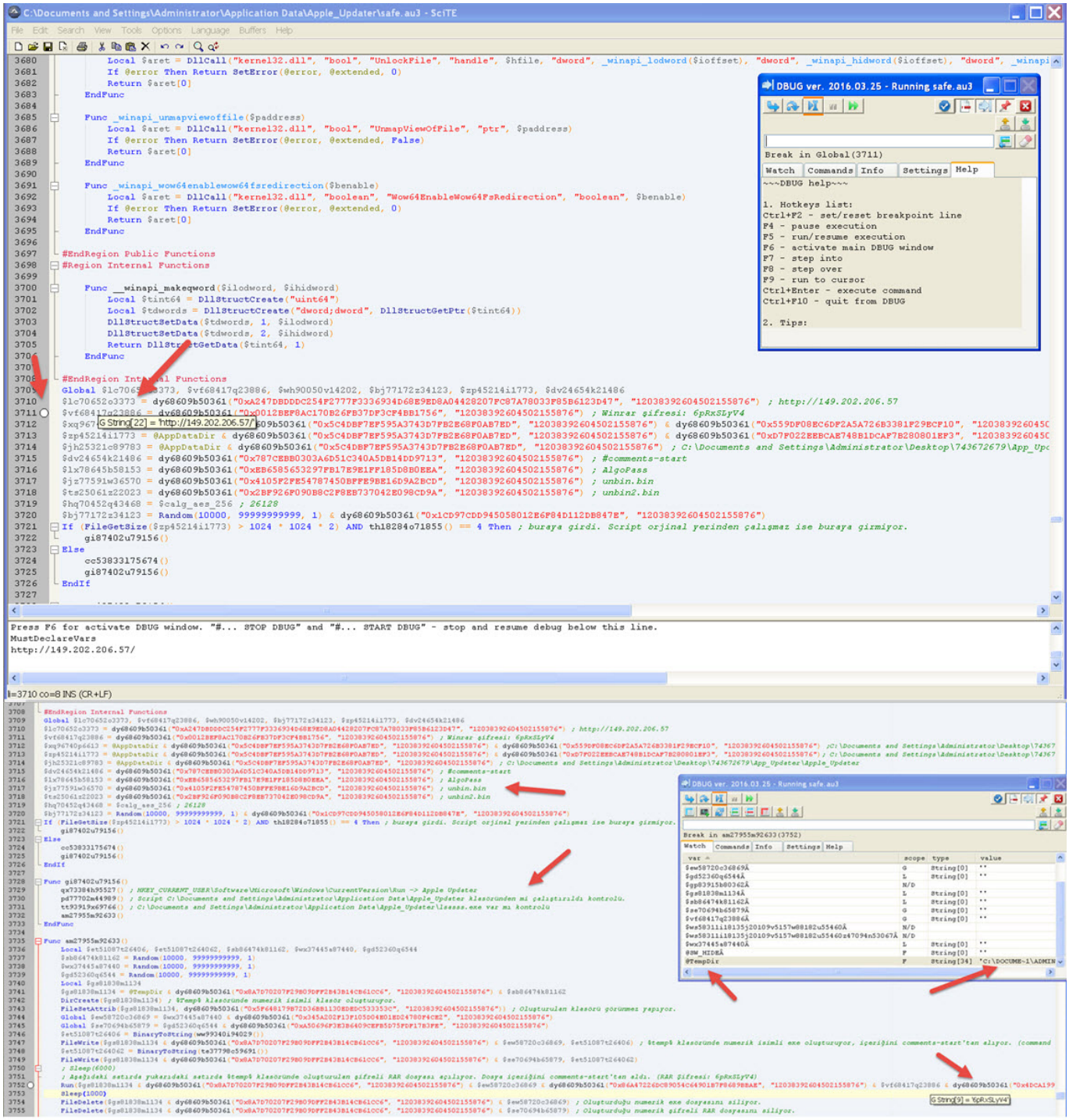
Hata ayıklama araçları (betikleri) arasında Dbug aracı, diğer araçlara kıyasla daha kullanışlı olduğu için onunla ilerleyebilirsiniz.

Dbug aracını kullanmak için öncelikle Auto IT script editörü olan SciTE aracını yüklememiz gerekiyor. Dbug aracının kurulum paketinden çıkan _Dbug.au3 dosyasını, analiz etmek istediğimiz safe betiği ile aynı klasöre koyduktan sonra safe betiğinin ilk satırına #Include “_Dbug.au3” satırını ekliyoruz. Bu işlemi gerçekleştirdikten sonra Dbug hata ayıklama aracını/betiğini çalıştırmak için başka bir eksiğimiz kalmıyor.

safe betiğini SciTE ile açtıktan sonra ilk olarak F5 (run/resume execution) tuşuna basarak Dbug aracının devreye girmesini sağlıyoruz. Fakat betiği çalıştırdığımızda, AutoIt kütüphanesindeki değişkenler ve fonksiyonlar ile betiktekiler çakıştığı için soruna yol açan bu değişkenleri ve fonksiyonları silmemiz gerekiyor.



Betiği sorunsuz bir şekilde çalıştırdıktan sonra gözümüze kestirdiğimiz bir satırın üzerine gelip F9 (run to cursor) tuşuna basarak program akışının o satıra kadar ilerlemesini sağlıyoruz. 3711. satıra geldiğimizde farenin imlecini (cursor) bir üst satırda yer alan $lc70652o3373 değişkenin üzerine getirdiğimizde, o değişkenin hangi değere (http://149.202.206.57) sahip olduğunu görebiliyoruz. OllyDbg aracında olduğu gibi F7 tuşuna basarak ilgili fonksiyonun içine girebiliyor, F8 tuşuna basarak ise (step over) fonksiyonun içine girmeden akışın (flow) devam etmesini sağlayabiliyoruz. Özetle Dbug aracı sayesinde adım adım fonksiyonların ne işe yaradığını öğrenerek, fonksiyonların yanına yorum (comment) da yazarak kısa bir süre içinde zararlı yazılımın/betiğin ne iş yaptığını kolaylıkla öğrenebiliyoruz.



Bu yazının son yıllarda AutoIt ile geliştirilen zararlı betikleri analiz etmede faydalı olması dileğiyle bir sonraki yazıda görüşmek üzere herkese güvenli günler dilerim.