Bad Bad USB

written by Mert SARICA | 3 November 2014
If you are looking for an English version of this article, please visit here.

Her yıl, Ağustos ayında, ABD'nin Las Vegas kentinde düzenlenen geleneksel Black Hat Bilgi Güvenliği Konferansı'nın sonuncusunda, Karsten NOHL ve Jakob LELL adındaki iki araştırmacı, BadUSB adında dikkat çekici bir sunuma imza attı.

Bu sunumda kısaca, USB'de yer alan mikrodenetleyici tarafından kullanılan donanım yazılımının (firmware) yamalanarak (patch) beklenenden farklı bir şekilde çalışması (hedef sistem üzerinde komut çalıştırma gibi) sağlanmış. Bunun için araştırmacılar öncelikle bu mikrodenetleyici tarafından kullanılan donanım yazılımını temin etmişler ardından Wireshark yardımı ile donanım yazılımı güncellemesi esnasında kullanılan komutları tespit etmişler. Daha sonra 2 aydan kısa bir süre içinde donanım yazılımını tersine mühendislik ile analiz ederek, orjinal donanım yazılımında yer alan ve kullanılmayan alanlara kendi komutlarını yükleyerek (notepad aç, şunu yaz, x sitesinden şu zararlı yazılımı indir ve çalıştır gibi) yeni bir donanım yazılımı oluşturup bunu USB belleğe yükleyip, işlemi tamamlamışlar. Bundan sonra hedef sisteme takılan USB bellek, veri depolamanın haricinde kullanıcının donanım yazılımı ile belleğe yüklemiş olduğu komutları çalıştırarak sistem ile etkileşime geçebilmiş.

Peki bunun daha önce üzerine yazı yazdığım ve yine hedef sistem üzerinde USB bağlantı noktasından takıldığı taktirde komut çalıştırmaya imkan tanıyan Teensy'den veya USB Rubber Ducky'den ne farkı var ? Pratikte pek bir farkı bulunmuyor. BadUSB ile gerçekleştirilen sosyal mühendislik testlerinde diğerlerine kıyasla hem sistemsel hem de görüntü itibariyle yakalanma/tespit edilme olasılığı görece biraz daha düşük olabiliyor. Maliyet açısından da bakacak olursak, BadUSB'nin 20$'lık Teensy'den, 40$'lık Rubber Ducky'den daha ucuza mal edilebileceğini görebilirsiniz.

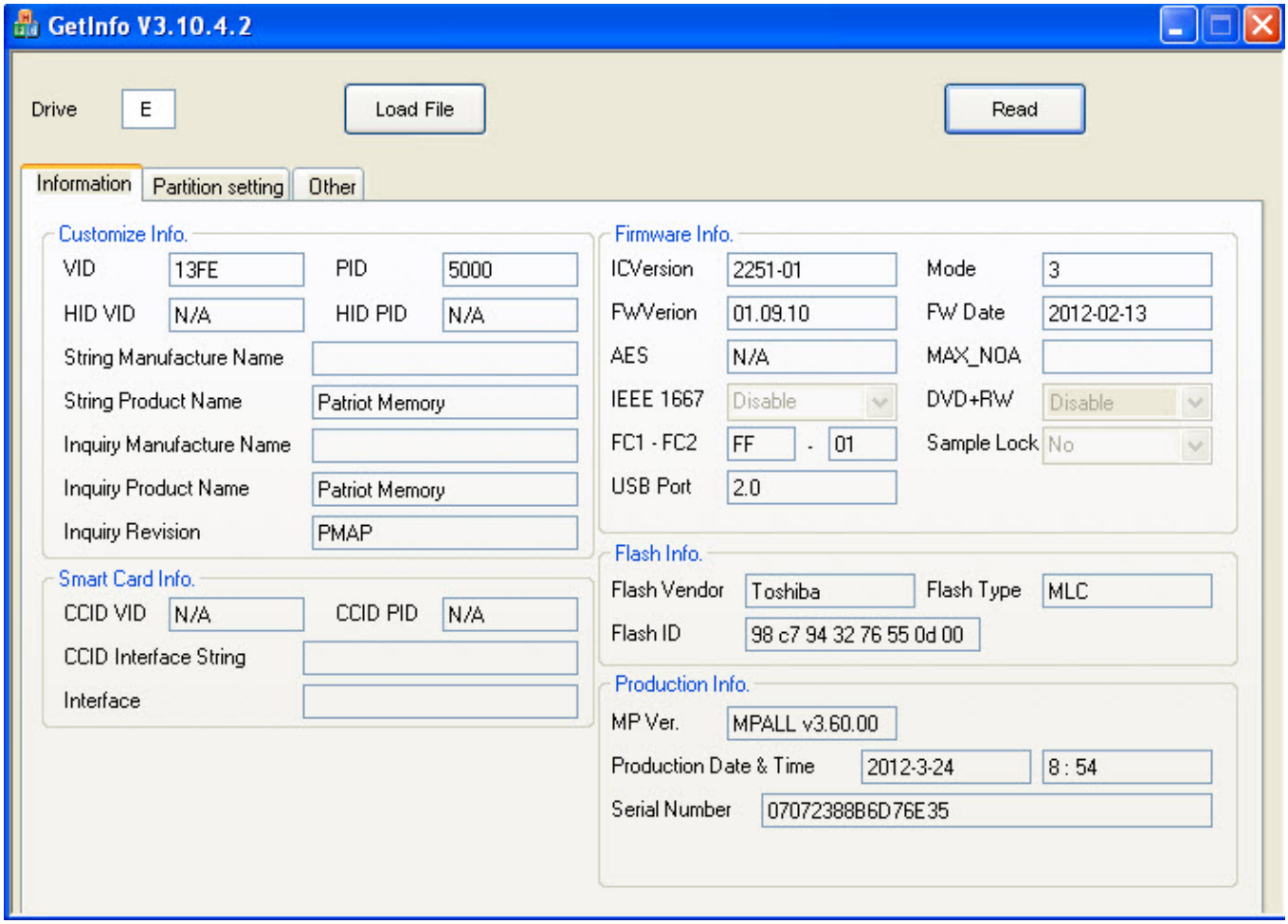
BadUSB ile ilgili çalıştırma yapan araştırmacıların web sitesini ziyaret edecek olursanız bu çalışmaya ait POC (proof-of-concept) kodlarını yayınlamadıklarını görebilirsiniz. Benim gibi ben de bir BadUSB oluşturmak istiyorum diyenlerin üzülmesine gerek yok çünkü Adam Caudill ve Brandon Wilson adındaki iki güvenlik araştırmacısı da benzer bir çalışma yaparak bunu Eylül ayının sonlarına doğru DerbyCon isimli Bilgi Güvenliği Konferansı'nda

sundular ve araştırma esnasında geliştirdikleri araçlarını da kaynak kodları ile birlikte GitHub'a yüklediler.

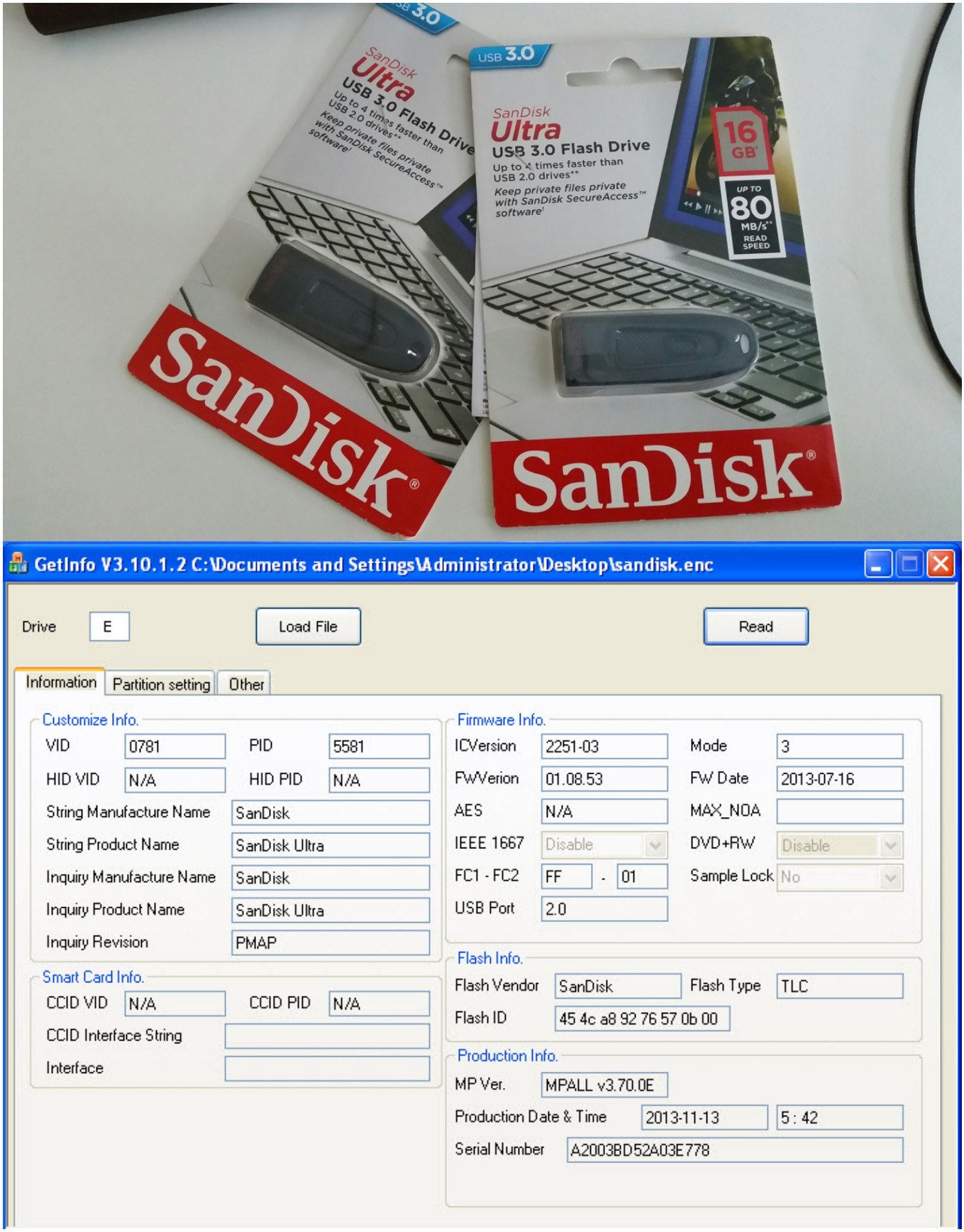
Sunum dosyasına ve kodlara baktıktan sonra ben de bir BadUSB oluşturmak için işe koyuldum. Araştırmacıların kullandığı Phison marka mikrodenetleyiciye sahip Patriot marka Xpress model USB bellek Türkiye'de olmadığı için Amazon'dan sipariş ettim.

Sunum dosyasına bakacak olursanız araştırmacıların Phison'un PS2251-03 modeli üzerinde çalıştıklarını görebilirsiniz dolayısıyla geliştirmiş oldukları aracın çalışabilmesi için kullanılacak olan USB belleğin bu model mikrodenetçiye sahip olması gerekmektedir.

USB bellek geldikten sonra Phison'un modelini GetInfo aracı (veya Chip Easy aracını da kullanabilirsiniz) ile kontrol ettiğimde modelin farklı olması nedeniyle hüsrana uğradım ve bu defa Phison marka PS2251-03 model USB bellek avına çıktım.

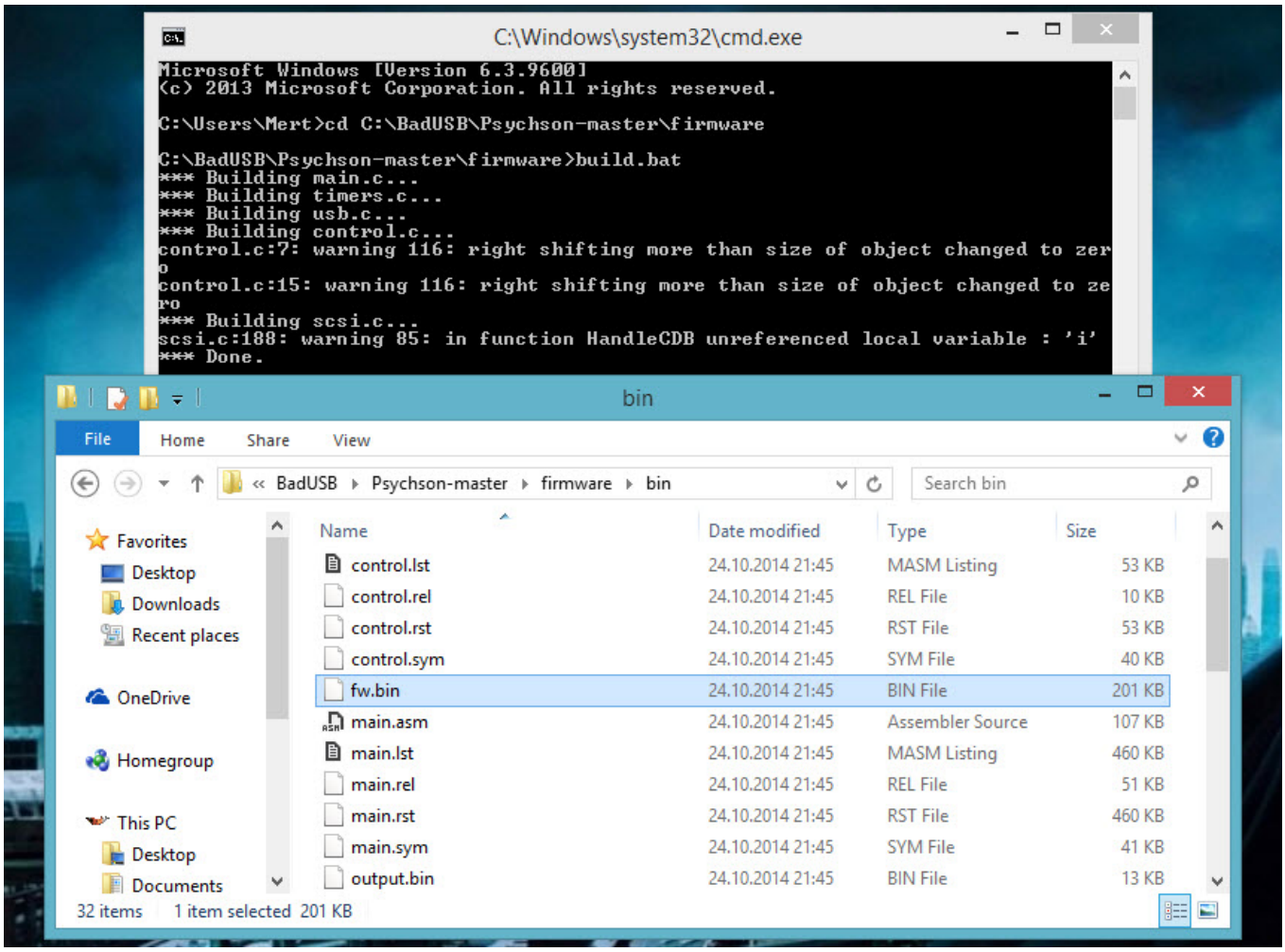


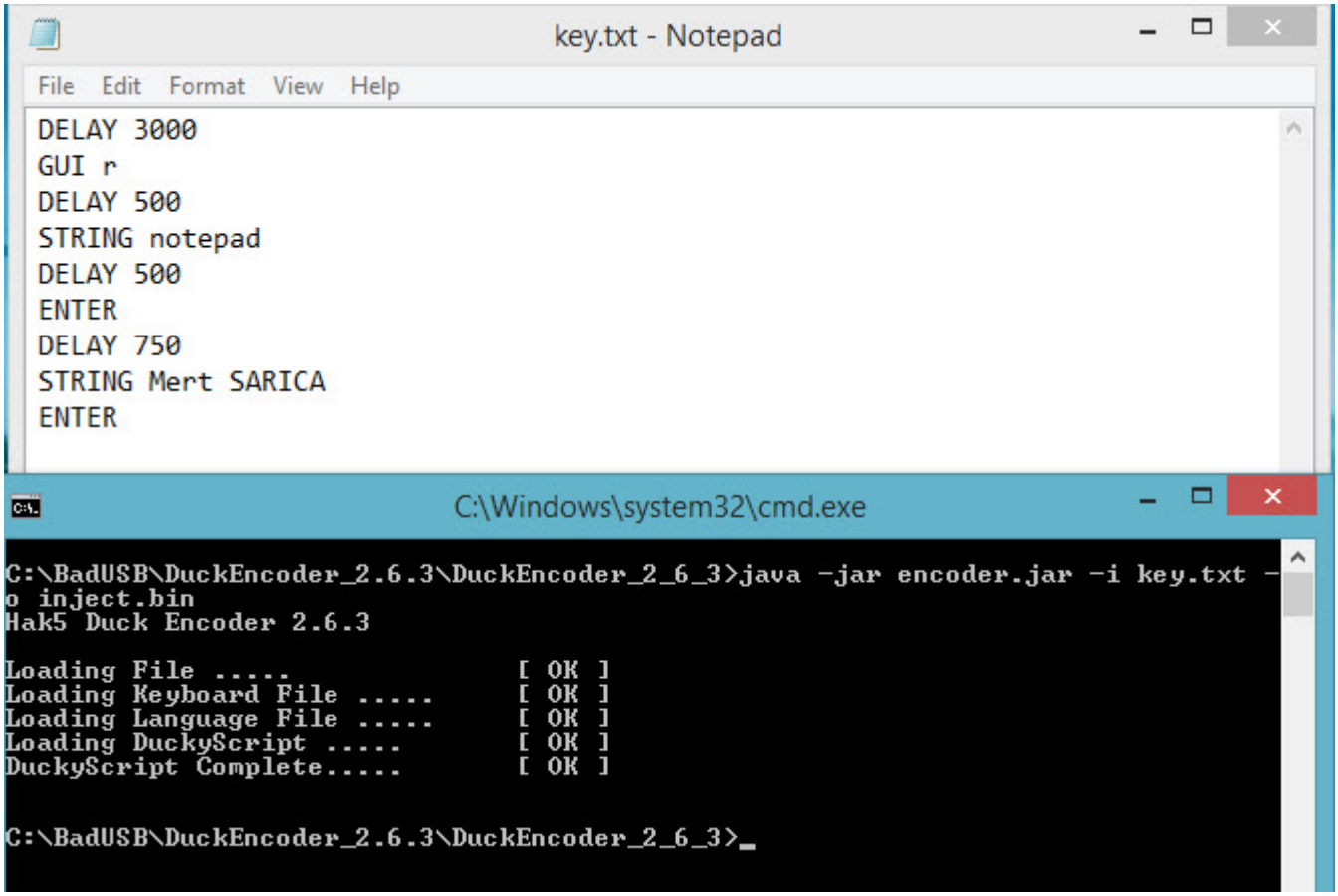
Benim gibi dünyada birçok kullanıcının ava çıkması ve araştırmacılara geri bildirimde bulunmaları sayesinde araştırmacılar, BadUSB olma potansiyeline sahip USB bellekleri bir listede toplamaya karar vermişler. Bu listeyi ara ara kontrol ederken, tesadüfen Teknosa'da gezerken gördüğüm Sandisk Ultra 16 GB USB belleği (SDCZ48-016G-U46) satın almaya (24 TL) ve modeline bakmaya karar verdim. Büyük bir hevesle paketini açıp, GetInfo aracı ile baktığımda Phison'un modelinin desteklenen model yani PS2251-03 olduğunu gördükten sonra GitHub sayfasında yer alan BadUSB yaratma adımlarına geçtim.



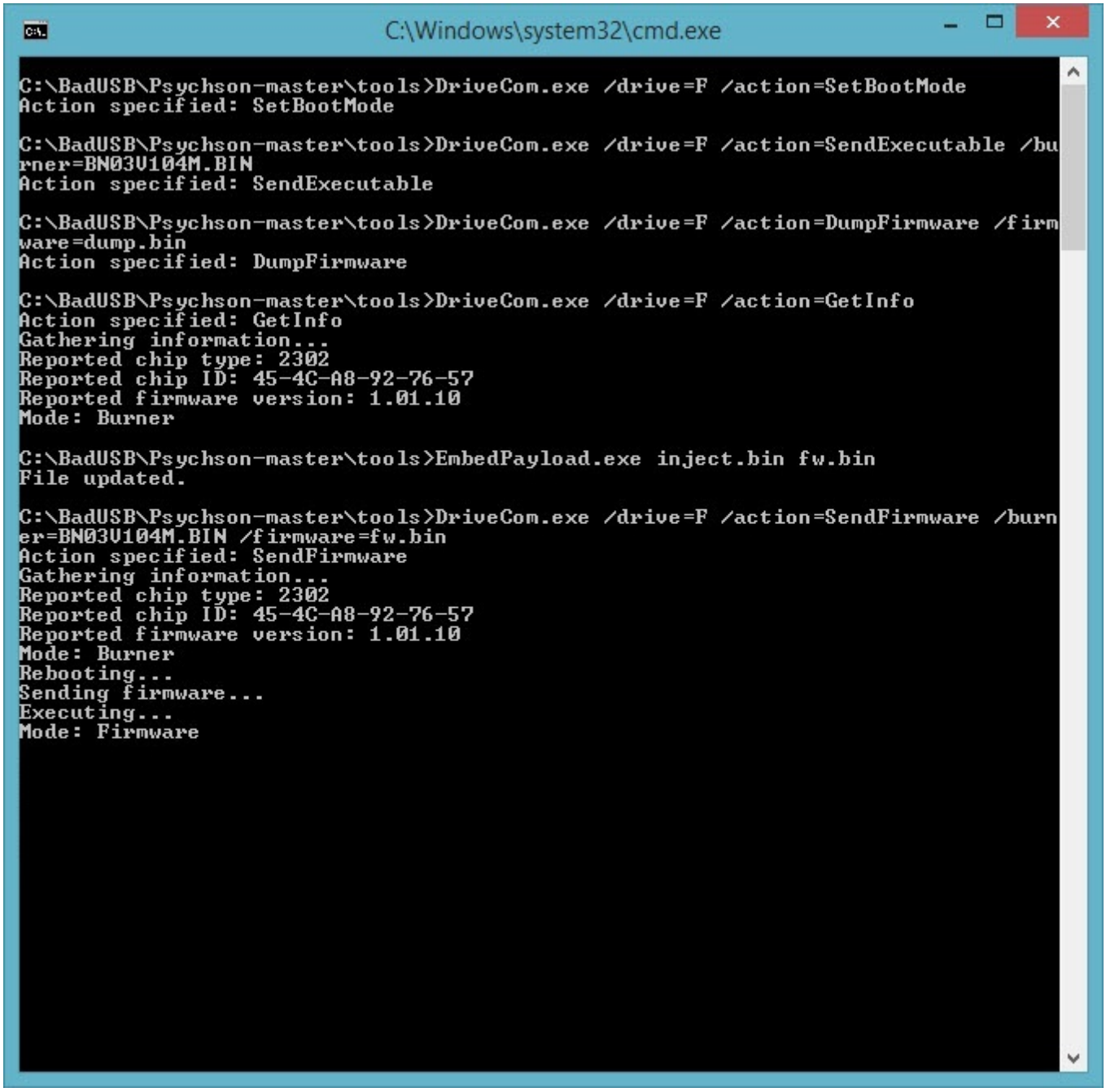
Adımlardan birinde yaptığım dikkatsizlikten dolayı aldığım bu diski çöpe atmak zorunda kaldım :) Ardından bu defa biraz daha temkinli davranarak iki tane daha Sandisk Ultra aldım ve yine bir dikkatsizlik sonucunda disklerinden birini daha çöpe atmak zorunda kaldım. Allah'ın hakkı üçtür diyerek BadUSB oluşturma adımlarını dikkatlice devam etmeye karar verdim. Donanım yazılımını

derledikten sonra sıra Ruby Ducky formatında bir komut kümesi oluşturmaya geldiğinde, Duckencoder aracı ile, çalıştır (run) -> notepad -> Mert SARICA yazan basit bir komut kümesi oluşturdum. (ReadMe dosyasında yer alan Running Demo 1 (HID Payload) başlığı altında yazılanları yaptım.)





Sonunda aşağıdaki tüm adımları başarıyla geçtikten sonra BadUSB oluşturmayı başardım :) Sandisk'in Ultra modelinde ne yazık ki donanım yazılımı bir defa güncelleme şansınız oluyor dolayısıyla şimdilik tek atışlık bir hakkınız var fakat bu konuda çalışmalar devam ediyor dolayısıyla elinizin altında sosyal mühendislik testlerinde kullanmak üzere bir tane bu marka model USB bulundurmanız faydalı olabilir.



Peki kurum olarak BadUSB'ye karşı hangi önlemleri alabiliriz diye soracak olursanız, kurum genelinde USB kullanımını yasaklayabilirsiniz. Bu mümkün değil ise de sadece IronKey gibi donanım yazılımı güncellemesine karşı imza kontrolü yapan ürünleri kurum genelinde kullanmayı tercih edebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: BadUSB'ye dönüştürülmüş USB ile ilgili hazırlamış olduğum videoyu aşağıdan izleyebilirsiniz.