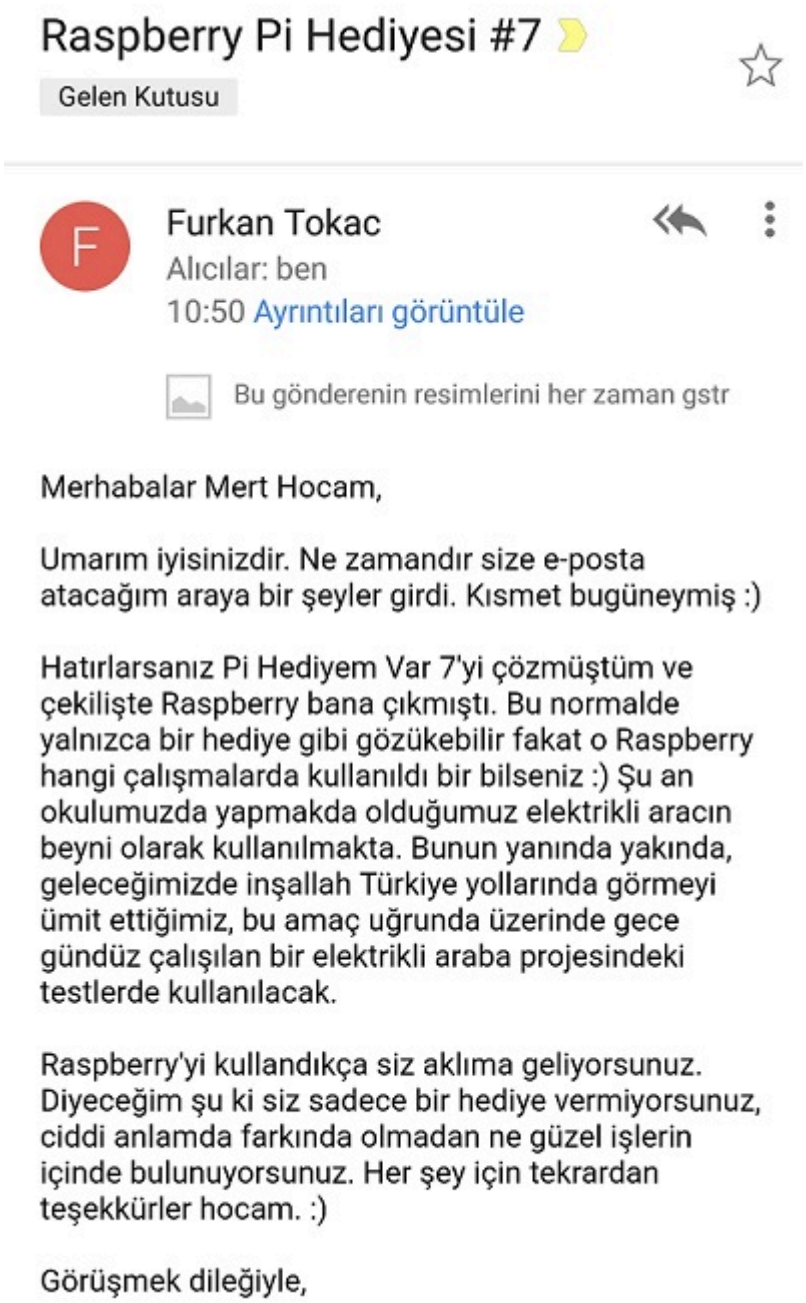
Pi Hediyem Var! #15

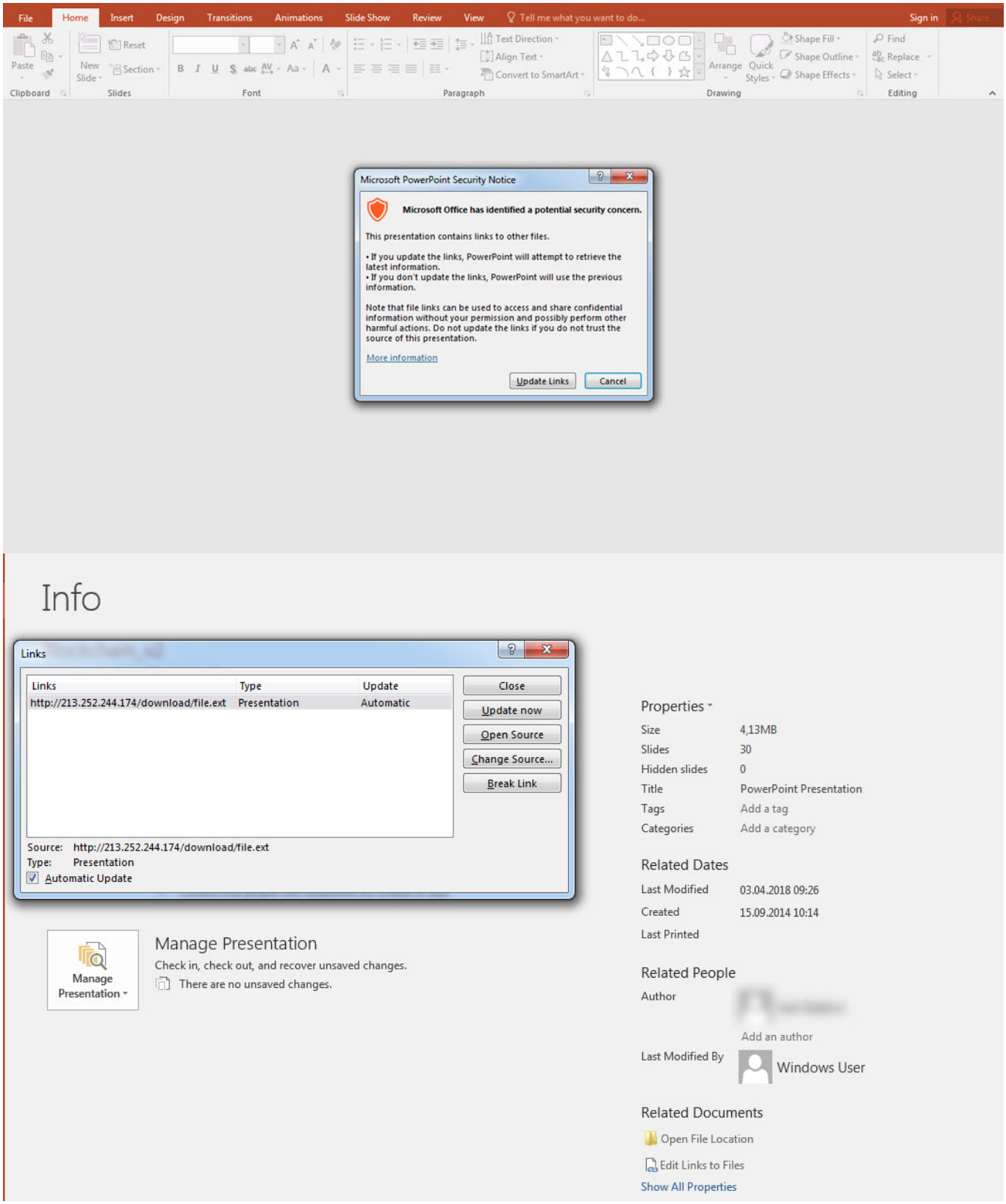
written by Mert SARICA | 29 June 2018

Yaz ayının ilk Pi Hediyem Var oyunu ile tekrar karşınızdayım. Önceki oyunlarda olduğu gibi bu oyunu da başarıyla tamamlayan üniversite öğrencileri arasında yapılacak çekiliş ile 2 adet Raspberry Pi 3'ü 2 öğrenciye hediye edeceğim. Bu oyunun Pi sponsoru olan FireEye Türkiye ekibine ve FireEye Türkiye Ülke Müdürü Ümit NADİM'e hem kendi adıma hem de tüm Pi Hediyem Var oyunseverleri adına teşekkür ederim.

Geçtiğimiz günlerde aldığım aşağıdaki e-posta ile hediye ettiğim Raspberry Pilerin siber güvenlik dışındaki projelerde de kullanıldığını öğrenmek beni oldukça mutlu etti, sizlerle de bu vesileyle bu e-postayı paylaşmak istedim. :)



Kurumsal SOME'de analist olarak görev yapan kahramanımız, kurumunun çalıştığı 3. parti firmadaki bir kişiden, 5 kurum çalışanına ekinde sunum dosyası (pptx) bulunan bir e-posta gönderildiğini ve güvenlik sistemlerinde alarm ürettiğini görür. Okuduğu tehdit raporlarında, APT gruplarının hedef kuruma sızmak için kurumun çalıştığı 3. parti firmaları hackleyerek onlar üzerinden kuruma sızma girişiminde bulunduklarını bilen kahramanımız, hızlıca bu dosyayı analiz etmeye ve bu APT grubu ile ilgili ipuçları elde etmek için işe koyulur.



Oyunu başarıyla tamamlamak için aşağıdaki tüm soruların cevaplarını, kod parçalarını ve ekran görüntülerini içeren kanıtları ile birlikte detaylı olarak açıklamanız gerekmektedir. Soruları yanıtlayabilmek için öncelikle https://www.dropbox.com/s/ie8yqg5s4xc16kw/ctf15.zip?dl=0 adresinden incelenmesi gereken şüpheli dokümanı indirmelisiniz. (zip şifresi: infected)

Yönergeler & Sorular;

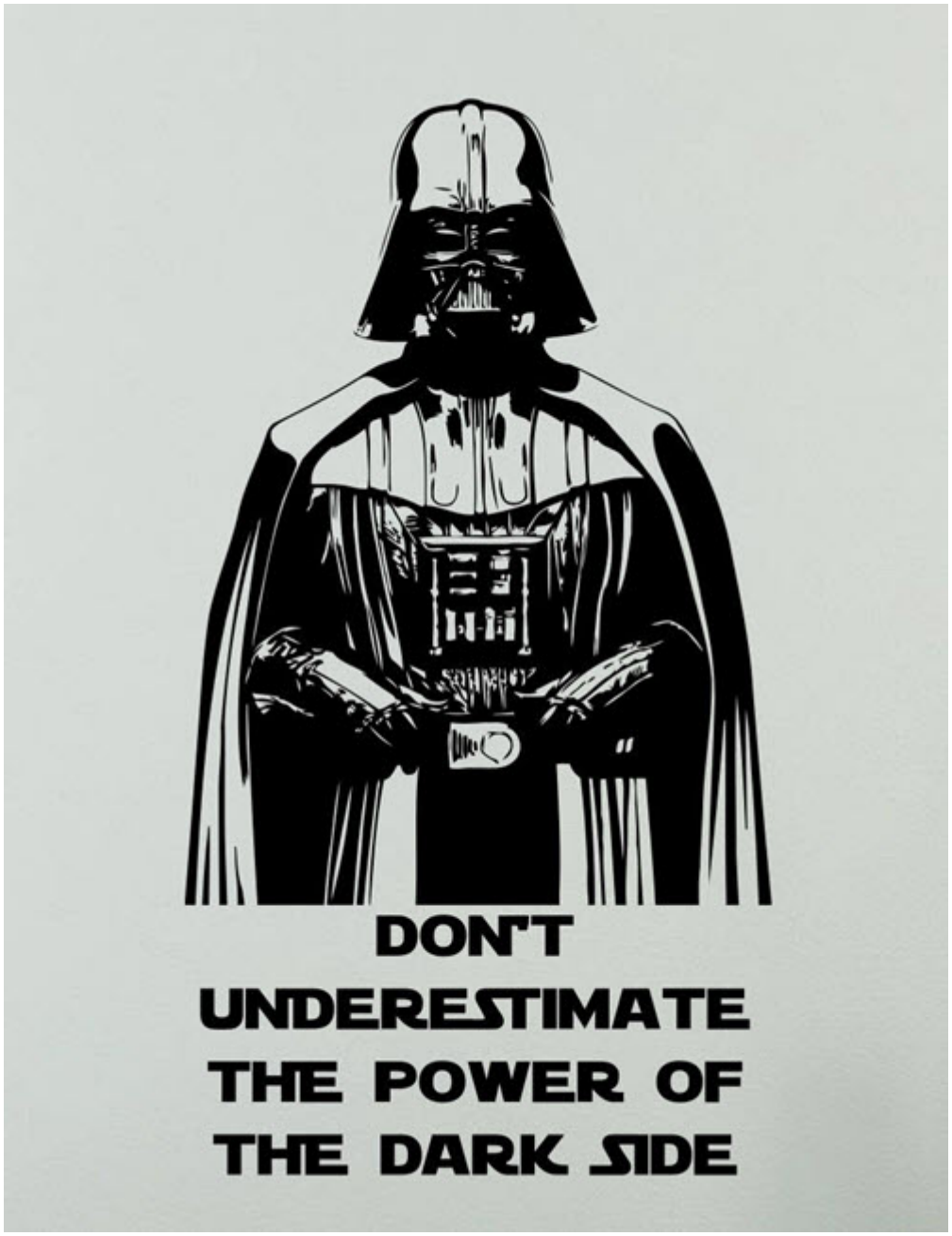
1. Şüpheli file.ext dosyasını ve HTTP trafiğini analiz ediniz.
2. Kabukkodunun türünü ve hangi araca ait olduğunu bulunuz.
3. Bellekten ve HTTP trafiğinden elde ettiğiniz ipuçları ile bu saldırının ardındaki potansiyel APT grubunu (birkaç bilgi sizi bir araştırma yazısına götürebilir) bulunuz.

Daha önce Raspberry Pi kazanmamış olup çekilişe katılmak isteyenler veya adını oyunu başarıyla tamamlayanlar listesine yazdırmak isteyenler, kanıtlarla (kod, ekran görüntüsü vs.) birlikte detaylı çözüm yolunu, adını, soyadını, yaşını iletişim formu üzerinden bana veya e-posta adresime 1 Temmuz Pazar Saat 23:59'a kadar iletmeleri gerekmektedir.

Oyunun çözüm yolunu içeren blog yazısı ilerleyen günlerde yayınlanacak olup, kazanan talihli bu sayfa ve Twitter hesabım üzerinden duyurulacaktır.

Not: Bu oyunu çözerken zararlı yazılım, kod analizi yaptığınızı hatırlatır, izole ve yaması güncel olan sanal sistem yazılımı (vmware, virtualbox vs.) ile çalışmanızı şiddetle tavsiye ederim.

Başarılar


DON'T
UNDERESTIMATE
THE POWER OF
THE DARK SIDE