Pi Hediyem Var! #19

written by Mert SARICA | 12 March 2021
If you are looking for an English version of this writing, please visit here.

2021 yılının ilk Pi Hediyem Var oyunu ile bir yıl aradan sonra karşınızdayım. Önceki oyunlarda olduğu gibi bu oyunu da başarıyla tamamlayan üniversite öğrencileri arasında yapılacak çekiliş ile 1 adet Raspberry Pi 4 ve 2 adet Raspberry Pi 3'ü hediye edeceğim. Bu oyunun Pi 4 sponsoru olan Keepnet Labs Türkiye Ülke Müdürü Erdinç BALCI'ya hem kendi adıma hem de tüm oyunseverler adına teşekkür ederim.

Oyunumuza gelecek olursam, uzun süredir siber güvenlik olay müdahale üzerine çalışan kahramanımız, organize siber saldırı grupları (APT) tarafından gerçekleştirilen siber saldırıları yakından takip etmekte ve teknik raporları inceleyerek bu gruplar tarafından kullanılan yeni taktik, teknik ve prosedürler konusunda bilgi sahibi olmaktadır.

Günlerden bir gün kahramanımızın çalıştığı kurumun vekil sunucusunda (proxy), bir çalışanın oluşturduğu web trafiğinde geçen EPUWBt3.png dosyası için PowerShell/Agent.QX güvenlik alarmı ürer. Aradan çok geçmeden bu defa aynı kullanıcının işletim sisteminde yüklü olan antivirüs yazılımında 8ROnVhd.png dosyası için PowerShell/Injector.D alarmı ürer.

Kısa bir süre önce APTv'nin 6. bölümünde dinlediklerini anımsayan kahramanımız bu alarmların hedefli bir siber saldırı kaynaklı olabileceğini düşünerek olup biteni çözmek üzere işe koyulur ve hikayemiz burada başlar.

Oyunu başarıyla tamamlamak için aşağıdaki tüm soruların cevaplarını, kanıtları (kod parçaları, ekran görüntüleri vs.) ile birlikte detaylı olarak açıklamanız gerekmektedir.
Soruları yanıtlayabilmek için öncelikle https://www.dropbox.com/s/syn4l1c6r35vsl4/ctf19.zip?dl=0 adresinden incelenmesi gereken şüpheli dosyayı indirmelisiniz. (zip şifresi: infected)

Yönergeler & Sorular;

1. EPUWBt3.png dosyasını analiz ederek zararlı kodu, bu kodu oluşturan aracı ve komuta kontrol merkezinin adresini bulunuz.
2. EPUWBt3.png dosyasının analizi esnasında elde ettiğiniz bilgiler ışığında 8ROnVhd.png dosyasındaki zararlı kodu ortaya çıkaran bir betik

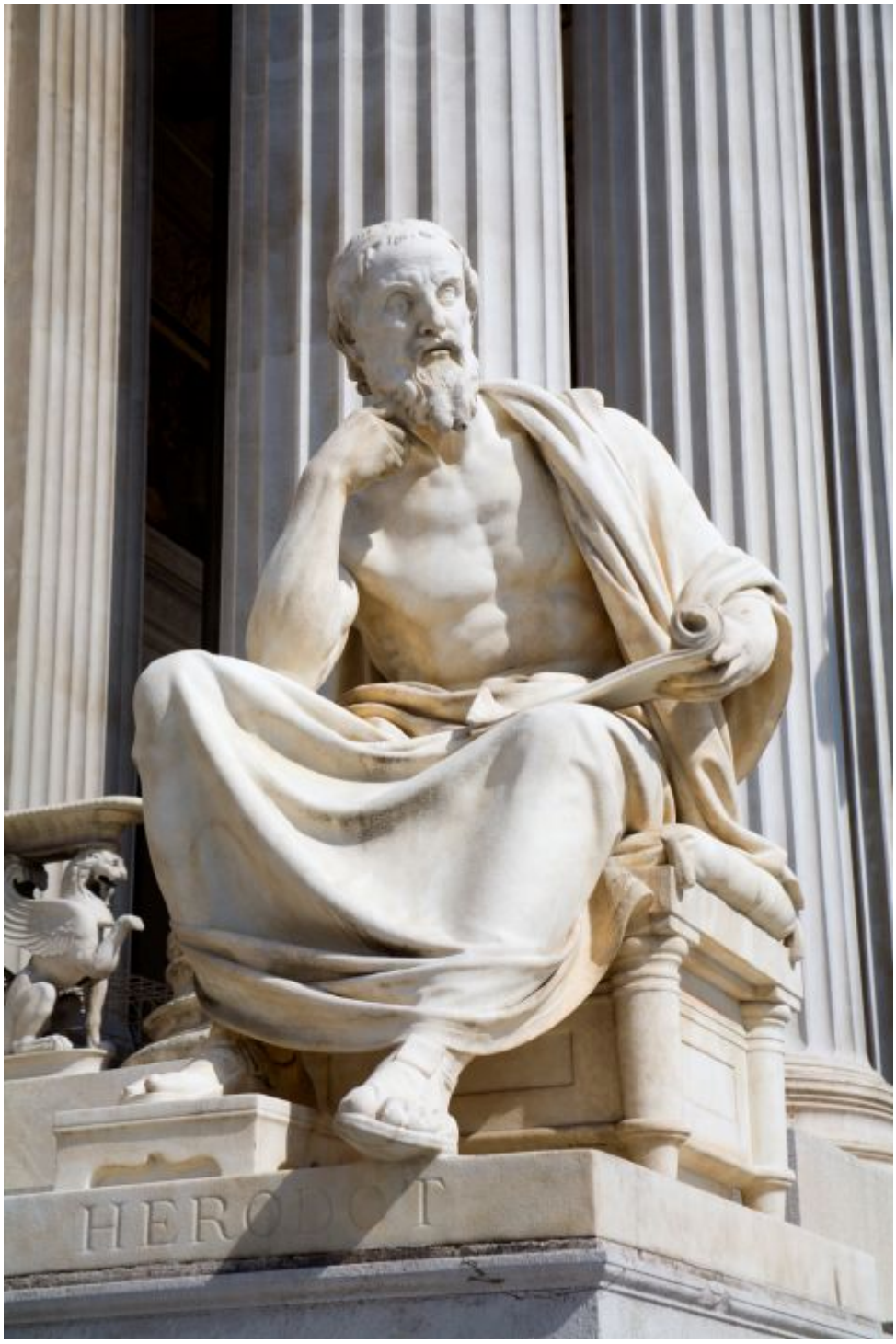
(script) hazırlayınız.

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 iletişim formu üzerinden bana veya e-posta adresime 14 Mart Pazar Saat 21:00'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



Herodotus tells how Demeratus, a Greek at the Persian court, warned Sparta of an imminent invasion by Xerxes: he removed the wax from a writing tablet, wrote his message on the wood underneath and then covered the message with wax. The tablet looked exactly like a blank one (it almost fooled the recipient as well as the customs men).