YARA Rule for the Executable files:

```
rule Ryuk_binary1 {
    meta:
          description = "Detects binary1.exe of RYUK ransomeware"
          author = "Sakahwat"
    strings:
         $s1 = "7S \i|9#X" ascii wide
         $s2 = "4Y6OjTi" ascii wide
         $s3 = "%\Y0aheA"
    conditions:
         any 1 of them

}
-------------------------------------------------------------------------------------------------
Ryuk_conhost {
    meta:
          description = "Detects conhost.exe of RYUK ransomeware"
          author = "Sakahwat"
    strings:
         $s1 = "API-MS-Win-Core-LocalRegistry-L1-1-0.dll" ascii wide
         $s2 = "VDM converting to fullscreen twice" ascii wide
```

```
          $s3 = "Finding Font file failed due to an error or insufficient buffer" ascii
wide
          $s4 = "Finding Font file failed due to an error or insufficient buffer"
     conditions:
          any 2 of them
```

```
Ryuk_CXYIJLO {
     meta:
           description = "Detects CXYIJLO.exe of RYUK ransomeware"
           author = "Sakahwat"
     strings:
          $s1 = "SYSTEM\CurrentControlSet\Control\Nls\Language\
InstallLanguage
0412" ascii wide
          $s2 = "Wow64DisableWow64FsRedirection" ascii wide
          $s3 = "vssadmin Delete Shadows /all /quiet"ascii wide
          $s4 = "vssadmin resize shadowstorage "ascii wide
          $s5 = "@protonmail.com"
     conditions:
         2 of them
```

```
Ryuk_EtuRifr {
     meta:
           description = "Detects EtuRifr.exe of RYUK ransomeware"
```

```
         author = "Sakahwat"
    strings:
        $s1 = "ReCreateDbcsScreenBuffer failed. Restoring to CP=%d" ascii wide
        $s2 = "Console init failed with status 0x%x" ascii wide
        $s3 = "vInvalid Parameter: 0x%x, 0x%x, 0x%x"
        $s4 = "RtlIntegerToUnicodeString"
        $s5 = "RtlIntegerToUnicodeString"
        $s6 = "RtlConsoleMultiByteToUnicodeN"
    conditions:
        all of them
```

```
 meta:
         description = "Detects NYPD.exe of RYUK ransomeware"
         author = "Sakahwat"
    strings:
        $s1 = "vssadmin Delete Shadows /all /quiet" ascii wide
        $s2 = "vssadmin resize Shadows shadowstorage" ascii wide
        $s3 = "@protonmail.com"
    conditions:
        3 of them
```

```
Ryuk_4VBTZWE4Ngo6 {
    meta:
         description = "4VBTZWE4Ngo6.exe of RYUK ransomeware"
```

```
        author = "Sakahwat"

    strings:

        $s1 = "runtime.(*gcControllerState).findRunnableGCWorker" ascii wide

        $s2 = "type..hash.struct { reflect.b bool; reflect.x interface {} }" ascii wide

        $s3 = "Token=b77a5c561934e089#~"ascii wide

        $s4 = "crypto/tls.(*clientHandshakeState).handshake" ascii wide

        $s5 = "SkipVerification" ascii wide


    conditions:

        any 1 of them
```

```
Ryuk_run-last {

    meta:

        description = "Detects run-last.exe of RYUK ransomeware"

        author = "Sakahwat"

    strings:

        $s1 = "runtime.(*gcControllerState).findRunnableGCWorker" ascii wide

        $s2 = "type..hash.struct { reflect.b bool; reflect.x interface {} }" ascii wide

        $s3 = "Token=b77a5c561934e089#~"ascii wide

        $s4 = "crypto/tls.(*clientHandshakeState).handshake" ascii wide

        $s5 = "crypto/tls.newConstantTimeHash.func1" ascii wide
```

conditions:

any 1 of them